S. HRG. 115–300

PREPARING SMALL BUSINESSES FOR CYBERSECURITY SUCCESS

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

APRIL 25, 2018

Printed for the Committee on Small Business and Entrepreneurship

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
30–630 PDF WASHINGTON : 2018

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP

ONE HUNDRED FIFTEENTH CONGRESS

JAMES E. RISCH, Idaho, *Chairman*
BENJAMIN L. CARDIN, Maryland, *Ranking Member*

MARCO RUBIO, Florida
RAND PAUL, Kentucky
TIM SCOTT, South Carolina
JONI ERNST, Iowa
JAMES M. INHOFE, Oklahoma
TODD YOUNG, Indiana
MICHAEL B. ENZI, Wyoming
MIKE ROUNDS, South Dakota
JOHN KENNEDY, Louisiana

MARIA CANTWELL, Washington
JEANNE SHAHEEN, NEW HAMPSHIRE
HEIDI HEITKAMP, North Dakota
EDWARD J. MARKEY, Massachusetts
CORY A. BOOKER, New Jersey
CHRISTOPHER A. COONS, Delaware
MAZIE K. HIRONO, Hawaii
TAMMY DUCKWORTH, Illinois

SKIFFINGTON E. HOLDERNESS, *Republican Staff Director*
SEAN MOORE, *Democratic Staff Director*

C O N T E N T S

Opening Statements

Witnesses

Alphabetical Listing

PREPARING SMALL BUSINESSES FOR CYBERSECURITY SUCCESS

WEDNESDAY, APRIL 25, 2018

UNITED STATES SENATE,
COMMITTEE ON SMALL BUSINESS
AND ENTREPRENEURSHIP,
Washington, DC.

The Committee met, pursuant to notice, at 3:30 p.m., in Room 428A, Russell Senate Office Building, Hon. James Risch, Chairman of the Committee, presiding.

Present: Senators Risch, Rubio, Ernst, Inhofe, Young, Rounds, Cardin, Cantwell, Heitkamp, Markey, and Booker.

OPENING STATEMENT OF HON. JAMES E. RISCH, CHAIRMAN, AND A U.S. SENATOR FROM IDAHO

Chairman RISCH. The Committee will come to order. Today we are going to have a hearing entitled Preparing Small Businesses for Cybersecurity Success. And I have a few remarks and then I am going to turn it over to the Ranking Member for his remarks. We will then hear from our distinguished panel. Thank you so much, all of you, for joining us.

Thank you, everyone, for coming today. This is a hearing on one of the most dire threats to small business and individuals in our Nation, the increasing number of attacks by cyber criminals. The same technology that enables small businesses to do business online and compete in the global marketplace also makes their sensitive information vulnerable to phishing schemes and ransomware attacks. Small businesses are especially vulnerable as about 71 percent of data breaches occur in businesses with fewer than 100 employees. Regrettably, many of these attacks are preventable and can be tied back to missteps made by a business' employees.

News of cyber attacks makes headlines each day, and we know that Russia, Iran, China, and North Korea are some of the biggest cyber hackers in the world. We have confirmation that Russia tried to interfere in our elections, and recent reports have been made public that they are compromising the information of individuals and small businesses in our country and the UK.

In recent years, the Russians have completely shut down Estonia's e-commerce, waged cyber war against Ukraine's energy grid, and they are constantly seeking to destabilize other countries. Additionally, North Korea has repeatedly attacked public and private entities in attempts to steal cryptocurrency to shore up their finances in the face of economic sanctions.

There are many bad actors out there and they grow in number and capability every day. Perpetrators vary from individuals to those directed by countries, putting small businesses in our country at great risk.

This issue hits especially close to home in a rural State like Idaho, where e-commerce is sometimes the only way to do business. That is why I have worked on three different pieces of bipartisan legislation to offer more tools to arm small businesses against potentially devastating cyber threats. The Main Street Cybersecurity Act will require the National Institute of Standards and Technology to disseminate a small business-friendly version of its renowned Cybersecurity Framework. This will better position small businesses to protect their assets, customers, and employees.

I have also introduced the Small Business Cyber Training Act to train the counselors at regional Small Business Development Centers throughout the country on educating entrepreneurs on protective cyber habits when they are first starting a new business, which will help them institute safe practices before the problem arises.

And just yesterday I introduced the Small Business Cybersecurity Enhancements Act to prepare the Small Business Development Centers to receive information on cyber threats and breaches from small businesses in the field when these incidents happen.

Cyber attacks are too frequently the last nail in the coffin for many small businesses, who are already facing an uphill battle to get started, get funded, and keep up with new regulations. I look forward to hearing from our witnesses today about their experiences with cyber threats and about what we can do to prevent these attacks.

I would like to welcome Mr. Daniel Castro, the Vice President of Information Technology & Innovation Foundation, and the Director of its Center for Data Innovation. Prior to ITIF, Mr. Castro worked as a scientist for the Software Engineering Institute and as an IT analyst for the Government Accountability Office. We look forward to his testimony, as he is named one of FedScoop's 25 Most Influential People Under 40 in Government and Tech.

I am also pleased to welcome Mr. Ben Toews from Hayden, a small town located in north Idaho. After starting with Bullet Tools, while still a student at Gonzaga University, Mr. Toews eventually worked his way up to become President of the company. He has helped Bullet Tools fend off a ransomware attack and has contributed to the company's 300 percent growth over the past five years. In addition to his full-time job, Mr. Toews is a member of the Idaho SBDC Advisory Council, assisting other small business owners and entrepreneurs. Mr. Toews, I look forward to your testimony. And, as a side note, Mr. Ranking Member, you would be interested to hear that when I sat in that seat, as the Chairman from the then majority party, I visited that business up there, and we were well entertained and enjoyed ourselves.

We also welcome Russell Schrader, the Executive Director of the National Cyber Security Alliance, and we welcome Ms. Gina Abate, President and CEO of Edwards Performance Solutions. Both of these will be further introduced by the Ranking Member Cardin.

Thank you for being here today with us. And now I would like to recognize Senator Cardin.

OPENING STATEMENT OF HON. BENJAMIN L. CARDIN, RANKING MEMBER, AND A U.S. SENATOR FROM MARYLAND

Senator CARDIN. Thank you, Mr. Chairman. There are days that I am looking for some road trips, so maybe we will look at visiting.

Chairman RISCH. Have you ever been west of the Mississippi River?

[Laughter.]

Senator CARDIN. Yes, a few times. A few times. Have you ever been on the Chesapeake Bay?

Chairman RISCH. I have. Many times.

[Laughter.]

Senator CARDIN. Good. We have a lot in common.

Chairman RISCH. I drink water from there.

Senator CARDIN. I am glad to hear it. The Chairman is a good friend and I appreciate his leadership on this Committee, and I particularly appreciate the fact that we are holding this hearing on preparing small businesses for cybersecurity success.

Cyber intrusions are a major problem, universal as well as in the United States. The Chairman is aware of this through our work on the Senate Foreign Relations Committee and his involvement on the Intelligence Committee. We know how active Russia is in cyber intrusions. North Korea, China, so many other countries.

I authored a report in January that talked about Mr. Putin's designs in regards to our democratic institutions, and one of the tools he frequently uses is cyber intrusions, in order to get as much information as he possibly can to compromise our system of government.

So we know we have major challenges in America with cyber intrusions. It is affecting our economy and it is affecting our privacy. We know that with Equifax and Target intrusions. We saw that with Facebook and the way that they handled personal information management, leaving a lot to be desired.

We also know that small businesses are a prime target of cyber attacks. There are 30 million small businesses that live with the understanding that they are at risk. An SEC report said that small businesses are the principal target for cyber crime, and we also know that 58 percent of the data breach victims were small businesses.

The challenge here is really why I am very pleased to have this hearing. For a small company that may not have a big staff for IT, does not have the margins to look at how to defend on cyber, and, quite frankly, probably has limited knowledge and understanding of the risks of cyber attacks, it is very difficult to be prepared against very sophisticated operators that are phishing for information, that could very well harm that company.

So we know that we have a challenge as to how we can help small businesses be prepared to deal with the realities of cybersecurity today, and part of that solution has to be education and knowledge and building capacity for small businesses, and I know we are going to get into that discussion today.

Mr. Chairman, I cannot let my opening statement go without bragging about the role that Maryland is playing in regards to cybersecurity. Maryland is home to the National Security Agency, the U.S. Cyber Command, NIST Cybersecurity Center of Excellence, Johns Hopkins University Applied Physics Lab, University of Maryland—I could go on and on and on. I am proud of the role that these institutions and the people who work there are playing in our national security in dealing with cybersecurity, and we have so many private companies that are now located in our state.

We recognize that the small business community is the driving force for our economy. That is where most jobs are going to be created. That is where most innovation is going to take place. So it is appropriate for us to figure out how we can better defend the small business community from the threats of cyber intrusion.

I welcome all four of our witnesses. The Chairman has given introductions for Mr. Castro and Mr. Schrader. Let me join in welcoming Ms. Gina Abate, the President and CEO of Edwards Performance Solutions, a certified women-owned small business in Elkridge, Maryland. Have you been to Elkridge, Maryland?

Chairman RISCH. I do not believe I have. Do they have elk in Maryland?

Senator CARDIN. Elkridge, Maryland, is a wonderful place. I pass it twice a day. I commute to Baltimore so I pass Elkridge twice a day. You are more than happy to go with me one day and we will stop by and visit.

Chairman RISCH. I want to see the elk.

Senator CARDIN. The company provides IT and cyber counseling services to commercial and government customers. She also chairs the Cybersecurity Association of Maryland.

And I am pleased that we also have Russell Schrader. He is the Executive Director of the National Cyber Security Alliance, the Nation's leading nonprofit public-private partnership that promotes cybersecurity and privacy education. Previously, he was Visa's first Chief Privacy Officer, where he oversaw privacy and data security policy.

So, Mr. Chairman, I think we have four very distinguished witnesses and I look forward to their testimony.

Senator MARKEY. Mr. Chairman, can I just interject to say that I think that Senator Cardin's opening statement could actually be used as a travelogue by the Maryland Chamber of Commerce, and I just wanted to compliment him for getting in just about every——

[Overlapping speakers.]

Chairman RISCH. As long as we are going to go down that road, I need to tell you a little bit about the Idaho National Laboratory that is becoming one of the lead agencies in America on cybersecurity. So I hope you will be able to visit the Idaho National Lab, in Idaho Falls someday.

In any event, thank you so much for coming, and we will just go right down the line, and any written testimony you will submit we will include in the record. We would ask you to keep the remarks at about five minutes, if you would, and we will go right down the line, starting with you, Mr. Castro.

STATEMENT OF DANIEL CASTRO, VICE PRESIDENT, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, WASHINGTON, DC

Mr. CASTRO. Chairman Risch, Ranking Member Cardin, members of the Committee, I appreciate the opportunity to appear before you today to discuss the opportunities to support small businesses as they seek to improve their cybersecurity practices.

As you know, small businesses face significant cybersecurity threats. In 2015, 42 percent of small businesses were victims of cyber attacks. In 2017, 58 percent of the confirmed data breaches involved small businesses.

Most small businesses are concerned about cybersecurity but they are not doing enough to protect themselves against these threats. One recent survey found that a third of small businesses are not taking any practice steps to protect against cyber threats, and half of them do not have a cybersecurity budget.

These risks present an existential threat to some small businesses, as firms can go bankrupt from the cost of responding to a cyber attack or from the lost revenue and customers resulting from a business disruption caused by a security incident. Moreover, these attacks are a drain on the U.S. economy, costing between $57 and $109 billion in 2016.

Therefore, I would like to discuss three steps Congress can take to improve cybersecurity practices.

First, one challenge that small businesses face is that they do not know what types of cybersecurity products and services they should be buying, or if they do know they cannot afford them because the per-user costs are too high. So companies that sell IT security products and services often use variable pricing, based on the number of users, or they require a minimum purchase amount. So these high per-user costs make the solutions unattractive or unfeasible for many small businesses.

So Congress should direct SBA to assist small businesses by establishing a cybersecurity cooperative, to create a large pool of willing buyers for various cybersecurity products and services, including cyber risk insurance. Participation in the cybersecurity co-op could be open to any small business, and depending on the level of interest, could be organized around particular regions or sectors.

The co-op could identify and evaluate cybersecurity products and services for its members and negotiate better rates for its users than they could get on their own. This would be a win-win. It would help small businesses get more value for their investments and also increase adoption of best-in-class cybersecurity tools. It would also lower the cost for those selling these products and services by reducing their customer acquisition cost.

Second, many small businesses cannot hire qualified cybersecurity professionals. Part of the problem, of course, is that there is fierce competition for individuals with these skills. In the United States, there are 40,000 cybersecurity jobs that go unfilled each year, and small businesses which often pay less than their larger counterparts have a hard time competing for this talent.

In addition, it is often impractical for a small business to hire a dedicated, full-time cybersecurity professional. Instead, they assign these responsibilities to an employee who works on these issues on

a kind of part-time basis. Unfortunately, virtually all of the cybersecurity certification programs are tailored for people who do this as their full-time job, so small business employees who only work on cybersecurity issues as part of their job do not pursue these credentials and they are often unqualified or under-qualified.

To address this problem, Congress should direct SBA to develop a low-cost, vendor-neutral certification program for small business employees who serve as their designated cybersecurity expert. The curriculum for the certification should be regular review, to ensure that it is accurate, comprehensive, and up to date, and SBA could authorize the professional certification organizations to actually provide the certification to those who successfully master the material. This certification would help small businesses assess whether they have staff qualified to handle cybersecurity issues, and ensure their investments in training are actually worthwhile.

And finally, small businesses will not have anyone who is properly trained—some of them will not—but these businesses still need to be able to mitigate common threats. So Congress should direct SBA to develop a free, online cybersecurity boot camp to provide small businesses the concrete steps they need to create a basic cybersecurity program to address the most critical threats facing small businesses. Participants would not be expected to come with any prior knowledge and they could repeat the boot camp as often as necessary. SBA would then be required to update the content regularly so that it contains information on both known as well as emerging threats.

Right now, the SBA offers one 30-minute class, but it is of poor quality. Some of the advice in the module is simply impractical. It has things like do not click on links in email, do not reply to unsolicited emails. This class also does not cover recent cybersecurity threats like ransomware.

Other government agencies, of course, offer resources, but many of their sites are not user friendly or they contain broken links. Sometimes the content is undated or outdated, most are redundant, and they overwhelm small businesses with unnecessary information.

Moreover, most of the resources either describe basic objectives, things like use stronger passwords, or they simply describe cybersecurity issues and terms. I think the analogy here is this would be like Ikea providing its customers one-pagers explaining the importance of not overtightening screws and pamphlets on the dangers of collapsing bookshelves, instead of giving them the actual step-by-step instructions of how to assemble furniture. Small businesses need this more practical guidance.

We need more leadership on this issue, and so I commend you for holding this hearing today. Thank you for the opportunity to be here and I look forward to answering questions.

[The prepared statement of Mr. Castro follows:]

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Daniel Castro

Vice President

Information Technology and Innovation Foundation (ITIF)

Before the

Senate Committee on Small Business and Entrepreneurship

"Preparing Small Business for Cybersecurity Success"

April 25, 2018

428A Russell Senate Office Building

Washington, DC

INTRODUCTION

Chairman Risch, Ranking Member Cardin and members of the subcommittee, my name is Daniel Castro, and I am vice president of the Information Technology and Innovation Foundation (ITIF), a non-profit, nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity, and director of ITIF's Center for Data Innovation. I appreciate the opportunity to appear before you to discuss opportunities to support small businesses as they seek to improve their cybersecurity practices.

CYBERSECURITY THREATS FACED BY SMALL BUSINESSES

Small businesses face significant cybersecurity threats: In 2015, National Small Business Association reported that 42 percent of small businesses were victims of cyberattacks.[1] The National Small Business Association found that, on average, cyberattacks cost small businesses approximately $7,000, and when their bank accounts were hacked, their average losses were approximately $32,000.[2] While small businesses generally face the same types of threats as larger businesses, small businesses experience a greater proportion of certain types of cyber incidents, such as malware and phishing attacks.[3] In addition, 58 percent of the confirmed data breaches in 2017 involved small businesses.[4]

Most small businesses are concerned about cybersecurity, but they are not doing enough to protect themselves against cybersecurity threats. One survey by CSID, a security firm owned by Experian, found that while a majority (58 percent) of small businesses are concerned about cyber threats, one-third were "not taking any pro-active steps to protect against cyber threats," and half "do not allocate any budget for risk mitigation services."[5] One reason for this lack of action is that many small businesses underestimate the potential risk they face from cyberattacks. For example, in one survey, a 57 percent of small businesses who had not suffered a cyberattack reported that they believed they could recover from a cyberattack within one month. Yet 60 percent of small businesses who had suffered a cyberattack reported that it took them more than a month to recover.[6]

These cybersecurity risks present an existential threat to some small businesses as firms can go bankrupt from the cost of responding to a cybersecurity incident or from the lost revenue and customers resulting from a business disruption caused by a cybersecurity incident. Indeed, the per user cost of these attacks is greater for smaller organization. In a recent study, Accenture compared the average cost for cybercrime per worker among organizations in the first and last quartile by number of employees. The study found that the average cost among the 25 percent of organizations with the fewest employees was four times as much as the average cost among the 25 percent of organizations with the most employees.[7] In addition, the Better Business Bureau found that more than half of small businesses would be unprofitable within a month if they were to lose permanent access to their essential data—such as would occur after a ransomware attack or hardware failure without data backup.[8]

OPPORTUNITIES TO ENHANCE CYBERSECURITY IN SMALL BUSINESSES

Cybersecurity threats present a major challenge for businesses. While both large and small companies face cybersecurity challenges, larger organizations are generally better equipped to handle cybersecurity threats than smaller ones. Indeed, few small businesses are taking the basic steps necessary to protect themselves from cybersecurity threats. One recent survey found that only 12 percent of small businesses reported having developed a cybersecurity response plan and only 21 percent reported providing security awareness training to employees.[9]

These cybersecurity vulnerabilities are a drain on the U.S. economy. According to the Council of Economic Advisors, cyberattacks cost the U.S. economy between $57 billion and $109 billion in 2016.[10] Therefore, Congress should take steps to bring small business cybersecurity practices up to par with larger organizations.

These steps should include:

1. Establishing a certification program for "part-time" cybersecurity professionals
2. Creating a cybersecurity boot camp for small businesses
3. Forming a small business cybersecurity co-op

Establish a Certification Program for "Part-Time" Cybersecurity Professionals

One problem small businesses face is difficulty hiring workers with the necessary cybersecurity skills and experience. This problem affects businesses of all sizes. By 2022, the International Information System Security Certification Consortium estimates that there will be a global shortage of 1.8 million cybersecurity workers.[11] In the United States alone, 40,000 cybersecurity jobs go unfilled every year.[12] The cybersecurity workforce shortage is likely to impact small businesses disproportionately, since small businesses tend to pay workers less than larger businesses and thus may have a harder time recruiting workers with highly sought-after cybersecurity skills.[13]

Moreover, in many cases it is impractical for small businesses to hire a dedicated, full-time cybersecurity professional, and so they instead assign these responsibilities to an employee without the proper training who works on these issues on a "part time" basis. Sometimes small business owners are themselves the individuals primarily responsible for managing cybersecurity threats, yet they are unfamiliar with the main cybersecurity risks facing their businesses. In one survey of owners, executives, and senior managers in small businesses, one-quarter had not heard of phishing attacks, one-third had not heard of ransomware, and almost half had not heard about point-of-sale malware that steals credit card data from customers.[14]

Organizations that lack employees with cybersecurity skills contribute to businesses failing to implement many important cybersecurity capabilities, such as multifactor authentication, network and endpoint forensics, and intrusion prevention systems.[15]

One way to address this skills gap is to provide better cybersecurity training to employees in small businesses. Existing efforts appear to be insufficient. For example, the U.S. Small Business Administration (SBA) offers only one cybersecurity training module through its online learning program. This 30-minute class offers participants a basic introduction to cybersecurity issues. However, most of the content is rudimentary to the point of being inconsequential. Moreover, some of the advice in the module is simply impractical, such as "Don't click on links in an email" and "Don't reply to unsolicited emails."[16] The module also does not cover recent cybersecurity threats, such as ransomware. Ironically, users can only access the training module if they install Adobe Flash, a multimedia platform for web content that has been removed or disabled from current versions of most Internet browsers.[17] To view the training content, users must click a link to install Flash on their computers, violating one of the module's key directives: "Do not allow any websites to install software on your computer."[18]

Other training programs offered for small businesses similarly often lack a high level of rigor because they do not adhere to any standard. While there are many certifications available for cybersecurity professionals, the vast majority of these certification programs are tailored towards dedicated, full-time cybersecurity workers. As such, obtaining these credentials requires more of an investment in time and money than is necessary or practical for small business employees who are only working on cybersecurity issues as a small part of their

job. To address this problem, SBA should work with existing professional certification organizations and the private sector to develop a low-cost, vendor-neutral certification program for small business employees who act as their company's designated cybersecurity expert. A panel of cybersecurity experts should regularly review the curriculum to ensure that it is accurate, comprehensive, and up-to-date. SBA could authorize any qualified professional certification organization, such as SANS, ISACA, ISC2, and CompTIA, that accurately assesses mastery of the curriculum to provide the certification. Such a certification would allow small businesses to assess whether they have someone qualified to handle cybersecurity issues and acquire necessary training. It would also ensure that they would not necessarily be forfeiting workers by overtraining them on cybersecurity skills, which may make them leave their existing job.

SBA should develop open educational materials for those who wish to complete the certification and make these training materials available directly to small business employees online. In addition, these resources could be integrated into in-person training offered by Small Business Development Centers or SBA-affiliated non-profits like SCORE, which provide assistance and mentoring to small businesses.

Create a Cybersecurity Boot Camp for Small Businesses

Some small businesses may never have a trained cybersecurity professional, but they still need instructions on the steps necessary to properly mitigate common cybersecurity threats. To better guide small businesses through the process of creating a basic cybersecurity program, SBA should develop a free online "Cybersecurity Boot Camp" for small businesses that provides participants the concrete steps they need to develop to identify, protect, detect, respond, and recover from cybersecurity incidents. The goal of the boot camp would be to raise the baseline level of security for any participant to address the most critical cyber threats facing small businesses. Participants would not be expected to come with any prior knowledge and they could repeat the boot camp as often as necessary. SBA should be required to update the curriculum regularly, so that it is contains information on known as well as emerging threats.

Virtually none of the existing resources the federal government makes available for small businesses offers this type of concrete, step-by-step guidance on how to implement the most effective cybersecurity tactics. Instead, most of the government-provided resources either describe basic objectives (e.g. "use strong passwords") or describe cybersecurity issues (e.g. defining terms like "distributed denial of service attack"). Small businesses need much more practical guidance. To understand why the federal government's current approach is ineffective, imagine if stores like Ikea provided their customers one-pagers explaining the importance of not over-tightening screws and pamphlets on the dangers of collapsing bookshelves, instead of step-by-step instructions on how to assemble furniture. Small businesses, especially those lacking IT professionals, need the detailed instructions.

Small businesses have limited resources to address cybersecurity threats, so the SBA should better curate the information presented to small businesses about how to address cybersecurity threats on its own site as well as that of its partners. While many different government agencies offer resources about cybersecurity for small businesses, they do not explain or describe how each resource differs from the others, contributing to information overload for small businesses. In addition to what the SBA provides directly and in partnership with the National Cyber Security Alliance, agencies such as the Department of Homeland Security, the National Institute of Standards and Technology (NIST), the Federal Communications Commission (FCC), and the Federal Trade Commission (FTC) all offer their own cybersecurity resources to small businesses.

Moreover, many of these sites are not user friendly, containing broken links or requiring users to navigate through multiple pages to find to the content. For example, one link on the FCC's website to its primary guide for small businesses leads to an error page with the message, "Your request looked malicious and has

been blocked."[19] In addition, many resources, such as the FCC's one-page handout "Ten Cybersecurity Tips for Small Businesses," are undated and others, such as the FCC's Small Biz Cyber Planner 2.0, are outdated.[20] Government provided cybersecurity resources should also be current, and agencies should be directed to withdraw or replace older materials to ensure small businesses are accessing accurate information.

SBA should promote its cybersecurity resources with all partners, including other federal and state programs as well as private sector initiatives, that work with small business, such as NIST's Manufacturing Extension Partnership Program, the Department of Commerce's Minority Business Development Agency, and the U.S. Chamber of Commerce.

Form a Small Business Cybersecurity Co-Op

One challenge small businesses face is that some cybersecurity products and services have high per-user costs when they purchase services for a relatively small number of employees. Often vendors offer variable pricing based on the number of users or require a minimum purchase amount. These high-per user costs make these solutions unattractive or unfeasible for many small businesses. One reason vendors charge more on a per-user basis for smaller companies is because of they have fixed customer acquisition costs.

For example, consider how businesses attempt to mitigate the threat of phishing attacks. Phishing attacks are a social engineering attack wherein an attacker attempts to impersonate a trusted entity, such as a financial institution or work colleague, to steal information from a potential victim by sending a message containing a malicious link or attachment that the unsuspecting target then opens. Between October 2013 and December 2016, the FBI's Internet Crime Complaint Center (IC3) tracked approximately 22,000 phishing attacks affecting U.S. businesses resulting in nearly $1.6 billion in losses, mostly from fraudulent bank transfers.[21] And a survey of small businesses found that 20 percent report having been victims of a phishing attack.[22]

Stopping these attacks is exceedingly difficult because the exact nature of the message changes frequently. Many businesses have found that one of the most effective ways to prevent these attacks is by conducting phishing simulations. Phishing simulations involve sending innocuous phishing attempts to employees using the same techniques employed by attackers. If employees fall for the rouse, rather than infecting their machine, they are given the opportunity to complete additional security awareness training. Unfortunately, cybersecurity vendors providing this type of phishing simulation service do not cater to small businesses, even though these businesses receive a disproportionate number of these types of attacks.[23]

SBA could assist small businesses by establishing a cybersecurity cooperative to create a large pool of willing buyers for various cybersecurity products and services, including cyber risk insurance. Participation in the Cybersecurity Co-Op could be open to any small business, and depending on the level of interest, could be organized around particular regions or sectors. The co-op could identify and evaluate cybersecurity products and services for its members and negotiate better rates for its users than they could get on their own. This would allow small businesses to get more value for their investments in cybersecurity and increase adoption of best-in-class cybersecurity tools.

CONCLUSION

Small businesses face many cybersecurity threats, and there is more the federal government can and should do to help small businesses succeed in addressing these threats. In addition to the recommendations outlined above, this committee, through its oversight, can insist that SBA provide small businesses timely and effective training materials about mitigating cybersecurity threats. However, these steps can ultimately fix only part of the problem. The greater challenge for the U.S. government is to reform its national cybersecurity policy to move away an emphasis on relative offensive capabilities and instead prioritize absolute defensive capabilities,

including prosecuting cybercrime. Such a change would require substantially rethinking how the U.S. government allocates funding for cybersecurity, how it releases cybersecurity research into the public domain, and how it works cooperatively with the private sector, through a reformed vulnerabilities equities process (for zero-day exploits) and expanded bug bounty programs.

REFERENCES

1. "2015 Year End Economic Report," National Small Business Association, 2016, http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.

2. "2015 Year End Economic Report," National Small Business Association, 2016, http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.

3. "2017 Cost of Cybercrime," Accenture, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

4. "2018 Data Breach Investigations Report," Verizon, 2018, https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

5. "Survey: Small Business Security," CSID, May 2016, https://www.csid.com/wp-content/uploads/2017/01/WP_SmallBizSecurity_2016.pdf.

6. "National Survey Reveals Most Small Businesses Unprepared for Cyber Attacks," Nationwide, 2016, https://www.nationwide.com/about-us/101316-cybersecurity.jsp.

7. "2017 Cost of Cybercrime," Accenture, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

8. "2017 State of Cybersecurity Among Small Businesses in North America," Better Business Bureau, 2017, https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

9. "Survey: Small Business Security," CSID, May 2016, https://www.csid.com/wp-content/uploads/2017/01/WP_SmallBizSecurity_2016.pdf.

10. "The Cost of Malicious Cyber Activity to the U.S. Economy," Council of Economic Advisors, February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

11. "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher," ISC(2), June 7, 2017, https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage.

12. Jeff Kauflin, "The Fast-Growing Job With A Huge Skills Gap: Cyber Security," Forbes, March 16, 2017, https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/.

13. Anthony Caruso, "Statistics of U.S. Businesses, Employment and Payroll Summary: 2012," February 2015, U.S. Census Bureau, https://www.census.gov/content/dam/Census/library/publications/2015/econ/g12-susb.pdf.

14. "2017 State of Cybersecurity Among Small Businesses in North America," Better Business Bureau, 2017, https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.

15. "Cisco 2018 Annual Cybersecurity Report," Cisco, 2018, https://www.cisco.com/c/en/us/products/security/security-reports.html.

16. "Cybersecurity for Small Businesses," U.S. Small Business Administration, n.d., https://www.sba.gov/course/cybersecurity-small-businesses/ (accessed April 20, 2018).

17. Gregg Keizer, "FAQ: How Apple, Google, Microsoft and Mozilla will eliminate Adobe Flash," ComputerWorld, July 31, 2017, https://www.computerworld.com/article/3211437/web-browsers/faq-how-apple-google-microsoft-and-mozilla-will-eliminate-adobe-flash.html.

18. "Cybersecurity for Small Businesses," U.S. Small Business Administration, n.d., https://www.sba.gov/course/cybersecurity-small-businesses/ (accessed April 20, 2018).

19. See link to https://www.fcc.gov/cyber/cyberplanner.pdf on page https://www.fcc.gov/cyberplanner (access April 22, 2018).

20. The FCC created the Small Biz Cyber Planner 2.0 in 2012.

21. "Business Email Compromise, Email Account Compromise, The 5 Billion Dollar Scam," Public Service Announcement, Federal Bureau of Investigation, May 4, 2017, https://www.ic3.gov/media/2017/170504.aspx.

22. "National Survey Reveals Most Small Businesses Unprepared for Cyber Attacks," Nationwide, 2016, https://www.nationwide.com/about-us/101316-cybersecurity.jsp.

23. "2017 Cost of Cybercrime," Accenture, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.

Chairman RISCH. Mr. Castro, have you communicated these same thoughts to the SBA?

Mr. CASTRO. No. Not out of this. We did do, actually——

Chairman RISCH. We will.

Mr. CASTRO. Okay. Great.

Chairman RISCH. Thank you. I appreciate your testimony.

Mr. Schrader, you are up next.

STATEMENT OF RUSSELL SCHRADER, EXECUTIVE DIRECTOR, NATIONAL CYBER SECURITY ALLIANCE, WASHINGTON, DC

Mr. SCHRADER. Thank you very much, Senator Risch, Ranking Member Cardin, distinguished Senators.

I appreciate the invitation. I know that this is an important topic.

I am the Executive Director of the National Cyber Security Alliance, founded in 2001. We are the leading neutral, nonprofit, private-public partnership devoted to strengthening America's cybersecurity through awareness and through education. We believe that cybersecurity is an economic and a security issue, as best addressed through collaboration between public and private partnership with industry, government, and consumers.

We bring together stakeholders to talk about cutting-edge issues, to execute highly hands-on, effective, broad-based education programs. Currently, one of our major partners is the Department of Homeland Security and our Board of Directors, which do represent leaders in technology, financial, insurance, and hospitality industries.

We have core education programs, including the National Cyber Security Awareness Month, which is October. It is co-founded and led with DHS; Data Privacy Day; STOP. THINK. CONNECT; and Lock Down Your Login, which is geared at congressional members, administration members right now; and the most recent addition to our portfolio, which is called CyberSecure Your Business, and I think that is the one that best aligns with what we are here to talk about today.

Today, as you pointed out, many businesses continue to think that they are too small to be a target of a cyber attack. These businesses lack the technical, the resources, the financial, and the legal things that they need to do to protect themselves. The NCSA's goal is to help entrepreneurs and small businesses across the country improve their cybersecurity, and we use targeted workshops that are aligned with the NIST Cybersecurity Framework.

We have translated that NIST Framework into simple language, and to create an introductory-level, in-person, interactive, three-hour-long workshop that we host in various cities around the country. It empowers non-technical businesses to improve their cybersecurity, and we talk to people like the local butcher, the barber, the local accountant, people who do not necessarily have any cybersecurity backgrounds, and they need to protect their highly valuable information and assets. They have some of the country's key IP, like employee and consumer data.

In addition, many of these small businesses are suppliers to large companies. They are part of the vendor management program. They are part of the supply chain of large businesses as well.

So our workshops are simple, they are actionable, and they have positive changes that small businesses can take to really move the needle on their own cybersecurity, and to reduce their own vulnerability to attack.

What we can do is we convene State attorneys general, SBA representatives, the FBI InfraGard, local FTC offices, chambers of commerce, Better Business Bureaus, and others to put on these programs and get small businesses to fill the rooms. Those small business attendees are armed with tangible resources to better secure their physical and their online assets, and they also have the awareness of the supports that are available to them throughout the country.

Now this is, right now, sponsored solely by sponsors from private industry, and these workshops are free to attend. I think seeing the trusted brands aligned alongside government agencies does send a clear message to businesses that the public and private sectors need to be joined together for the benefit.

We also supplement these in-person workshops with monthly CyberSecure Your Business webinars, which are hosted on the second Tuesday of every month between 2 and 3 p.m., Eastern time.

Now the NCSA applauds the Federal agencies' roles in providing small businesses with the resources and tools they need to become cyber secure. In addition, we promote these within the organizations with our own materials, and we continue to support cross-agency and cross-public-private collaborations such as the one we have, the DHS, in order to do this. But we need more support dedicated to helping businesses prepare, and I look forward to the opportunity to talk with the community in ways that NCSA works with this Committee and other stakeholders in order to improve this very useful program.

And I point out, Mr. Chairman, based on the earlier conversation, that we had already scheduled one of these trainings to take place in Boise in the next coming months. We will talk about Elkridge at another time.

[The prepared statement of Mr. Schrader follows:]

Testimony of Russell Schrader

Executive Director, National Cyber Security Alliance

U.S. Senate Committee on Small Business & Entrepreneurship

"Preparing Small Businesses for Cybersecurity Success"

April 23, 2018

Founded in 2001, the National Cyber Security Alliance (NCSA) is the leading neutral nonprofit, public-private partnership devoted to strengthening America's cybersecurity through awareness and education. We believe cybersecurity is an economic and security issue best addressed through collaboration among industry, government, academia, consumers and NGOs. We bring together stakeholders to discuss cutting-edge issues and create and execute high-quality, large-scale education and awareness programs. Currently, our primary partners are the U.S. Department of Homeland Security (DHS) and our Board of Directors, representing leaders in the technology, financial, insurance, hospitality and telecommunications industries.

NCSA's core educational and awareness campaigns include National Cyber Security Awareness Month (co-founded and led with DHS), Data Privacy Day, STOP. THINK. CONNECT.™ and Lock Down Your Login. The most recent addition to NCSA's portfolio, and the one I think best aligns with the topic of this hearing, is our CyberSecure My Business™ initiative.

Today, many businesses nationwide continue to think they are too small to be a target of a cyberattack. These businesses often lack the human, technical, financial and legal resources their larger counterparts have at their disposal. NCSA's goal is to help entrepreneurs and small businesses across the country improve their cybersecurity through targeted workshops aligned with the NIST Cybersecurity Framework. We also tailor our programs to include compliance information for state data breach notification law.

As the CyberSecure My Business cornerstone, we've translated the NIST Cybersecurity Framework into simple language and have incorporated it into our introductory-level, in-person, highly interactive three-hour workshop hosted in communities throughout the U.S. The workshop is designed to empower non-technical small businesses to improve their cybersecurity. We target companies like the local butcher, barber, pediatrician, etc. who may not have information security backgrounds, nor perhaps someone on their staff with this capability. They still, however, need to protect their highly valuable information and assets. It is important to keep in mind that they have some of the country's most prized intellectual property to protect – like employee and customer data. In addition, many are suppliers of goods and services to larger organizations, including the federal government. CyberSecure My Business workshops share actionable steps organizations can take to make positive changes in their behaviors, processes and technologies to reduce their vulnerability.

The workshops are held in six to eight locations nationwide each year and are intended to empower non-technical, small businesses to improve their cyber posture. Each in-person training can reach 125

businesses. We convene state Attorneys General, the U.S. Small Business Administration, the Federal Bureau of Investigation's InfraGard, Federal Trade Commission, law enforcement, Chambers of Commerce, Better Business Bureau chapters, Small Business Development Centers and others. Small businesses not only leave armed with tangible resources they can use to better secure their digital and physical assets, they also gain an awareness of the support network available at their fingertips.

The program is supported by national sponsors from private industry, which enables the workshops to be conducted at no cost to the business. Seeing trusted, national brands alongside respected government agencies sends a clear message to businesses – that the public and private sectors have joined together for the their benefit. This public/private effort is critically important and a fundamental component of our CyberSecure My Business programing because it brings various stakeholders and support systems in one room to share a dialogue along with local, state and national resources.

In the five workshops we have completed to date during our national CyberSecure My Business tour, a total of 615 people have joined us, averaging 123 attendees per workshop.

We also supplement our workshops with a CyberSecure My Business webinar series, featuring federal and private sector partners in collaboration with NCSA staff. Since the inception of the webinars in October 2017, we have had 3,050 participants internationally. The webinars are hosted on the second Tuesday of the month from 2:00 - 3:00 pm ET.

NCSA applauds the role federal agencies play in providing small businesses with the resources and tools they need to become cybersecure. In addition, NCSA continues to promote these resources to the community along with our own materials. We will also continue to support cross-agency and public-private collaboration when it comes to the development of these much-needed cybersecurity resources and training. Cybersecurity is a shared responsibility, and the more work that is done on a national level to deploy standards and to shift liability to the merchants, the more support we need to dedicate to helping the businesses prepare. I look forward to the opportunity to talk with the committee about ways NCSA works with stakeholders to fund and deliver these much-needed and highly useful programs in connection with the enforcement actions and strong protective stances you continue to take.

Chairman Risch, Ranking Member Cardin and distinguished Senators, thank you for the opportunity to present this testimony.

Chairman RISCH. Thank you so much.
Ben, you are up.

STATEMENT OF BEN TOEWS, PRESIDENT, BULLET TOOLS, HAYDEN, ID

Mr. TOEWS. Right. Chairman Risch, Ranking Member Cardin, Senators, thank you for the opportunity to testify today. My name is Ben Toews, President of Bullet Tools. My degree is in international business, not information technology. Managing the techy side of my business was a necessary evil. I created our network, got everyone connected, and did the troubleshooting and training. Once I found competent IT people I handed over the reins and never looked back.

So what qualifies me to testify, now that you know I am not a computer genius? In short, having my business hacked with ransomware and surviving. Let us look at my company as a case study. Before the cyber attack, I think most would say that we were well protected. Our first line of defense was a hardware firewall, our second line of defense was a domain controller with centrally administrated usernames and passwords, and the third line of defense was Microsoft Security Essentials. Our fourth line of defense was informal training of users on good internet and email practices, and our final line of defense was an offsite backup of our financial and inventory data, on a daily basis.

Immediately before the attack, we set up a new computer without antivirus software. A new user with no password then plugged it into our network. This made us vulnerable and the hackers executed ransomware that encrypted every file that the new user had access to. When we discovered the attack and saw the ransom note we used our cell phones to find online resources to help clean and restore our system. All of our shared network files were encrypted but only one user was compromised.

We restored the financial and inventory backups to the network, and most of our company was back to normal in three to four hours. We were lucky. Without the offsite backup, we would have been virtually dead. We did lose some files, but none crucial to our operations. We now have additional security measures in place, along with daily offsite backups of all folders.

So what lessons did we learn? I think that learning from others' mistakes is a lot less painful than making them yourself. That is why I am here to encourage you to help small businesses learn from my experience.

There is an example that compares well to the situation. At the beginning of the Second World War, the British were concerned that the Luftwaffe would attack, millions of Londoners would flee, and the country would be paralyzed. Thankfully, that scenario did not play out.

JT MacCurdy, in The Structure of Morale, described the effect of the blitz as splitting the population into three groups. One, the people killed by the bomb. A harsh fact: dead people do not spread panic. Two, the near misses. They feel the blast, see the destruction, it may result in shock and a preoccupation with the damage. Three, the remote misses. These people hear the sirens and explo-

sions. For them, the experience is remote. The result? A feeling of invulnerability.

Small business falls into these three categories: those that have been hacked and did not survive, those that have been hacked and survived, and those that have not been hacked. The first category is not going around advertising it, and want to forget it ever happened. The second category is likely more prepared, and unless it happened quite recently, have set up a very secure computer system, or gone back to flip phones and faxes. The last category is the remote miss group. They have heard about companies being hacked but nothing has hit close enough to get their attention. This group, the majority, is going to need the most help. Cyber criminals have realized that small, easy targets can be very lucrative.

I do not believe that government programs are the best way to solve issues like cyber crime but they are very useful in creating an environment that encourages great solutions in the private sector. This is accomplished by informing and empower small businesses, and the SBDC as an excellent organization to accomplish this.

The Idaho SBDC helped my company write our initial business plan, obtain funding, and weather the storms of growing a business over about 18 years. I now sit on the Advisory Board of the Idaho SBDC.

The SBDC has some good resources in place to help prevent or mitigate the devastating effects of cyber attacks, including vulnerability assessments and other tools. These resources need to be actively leveraged and promoted to the small business community. I believe this should be done through public service-type announcements sent through various social media platforms targeting small businesses. I think we are all aware now that social media has the necessary info to do so.

Federal agencies also need to be encouraged to collaborate with SBDCs and promote them as a resource. There are nearly 1,000 SBDC locations providing boots on the ground, coaches across the country, who can educate those at risk, as well as help equip the small businesses that provide cybersecurity services and can provide a truly scalable solution.

When dealing with IT, small business owners are wary. It is hard to know what the people you hire are doing, and if they should be trusted. The solution is standardized, reputable certifications for cybersecurity professionals.

I hope that my testimony will help make a difference in combating cyber attacks, and it has been an honor speaking with you today.

[The prepared statement of Mr. Toews follows:]

U.S. Senate Committee for Small Business & Entrepreneurship

"Cybersecurity" Hearing April 25th, 2018

Testimony:
Ben Toews
President
Bullet Tools - Hayden, ID

Thank you Chairman Risch, Ranking Member Cardin and distinguished Senators for the opportunity to share this testimony with you.

I'd like to start by explaining what specifically qualifies a small business owner/operator like myself to speak on this subject. My degree is in International Business, not Information Technology. Managing the techy side of my business was a necessary evil during the early days of my company but I learned a lot. I created our business network, figured out how to get everyone connected and did my share of troubleshooting and training people to use and protect their computers. As soon as I found people who were capable, experienced and undoubtedly more passionate about IT then I was, I handed over the reins and never looked back.

Not that I don't recognize the importance and benefit of the amazing organization, information processing, communication and collaboration that technology allows, I really do appreciate it and leverage it. My business spends roughly the same amount on IT related purchases as we do on R&D which is the lifeblood of our business. That doesn't mean that I love the nitty gritty details of how it all works. I'm guessing a lot of you are like me.

So, what qualifies me now that you know that I am not a computer genius, a hacker or a cyber security specialist? In short -- having my business hacked with ransom ware and surviving it on June 4th of last year. Let's look at our company as a sort of case study by analyzing our security measures before and after the attack along with how we recovered with relatively little damage.

Security plan BEFORE the attack:

Our first line of defense was a hardware firewall which is very secure but, to make our VOIP phones work we had to open numerous ports which acted as open doors. Our second line of defense was a domain controller with centrally administrated user names and passwords. The third line of defense was Microsoft Security Essentials on each desktop although it was not updated regularly. This is known to be ~90% secure if up-to-date. Our fourth line of defense was informal training of users of good internet and e-mail practices (don't respond to Nigerian princes who request bank account information no matter how much money they are offering you, or send wire transfers overseas without a verbal okay). Our fifth and final line of defense was to back-up our Financial/Inventory data offsite on a daily basis.

Friday before the attack:

We set-up a new computer without any antivirus software (no security guard), Set-up new user with no password (unlocked door), a brand new non-updated version of windows 7 pro (blinking arrow pointing to entrance) and plugged it into our network (an illuminated path to the unlocked safe).

What happened (as near as we can tell)

The non-updated version of Windows was viewable as a potential vulnerability. Once they had our IP address they could tell we had a remote desktop activated. They likely used a brute force user name attack to find out if any users had no password protection then used the user without a password to execute a piece of ransom ware on our server which encrypted every file that the user had access to and placed a ransom note in every folder the user had access to. We discovered this on Monday morning.

Recovery

We discovered we had been attacked and 1st had everyone turn off computers and unplug from network We had to analyze what had happened to determine how widespread and ongoing the issue was. After seeing the ransom note we used our cell phone browsers to find reputable online security companies with utilities that could identify and possibly help us restore our system. We cautiously booted one system at a time and searched for encrypted files and found that only our shared network folders and the files on the remote desktop account of one user were encrypted.

As each system was booted we installed Malwarebytes and ran a full scan where we discovered that the new computer had over 300 malware/virus files. Everything else was mostly clean. Computers using outlook often had some slight issues. We deleted the user, backed up the infected files on a separate hard drive and deleted from networked folders, updated windows on the new computer and all others then restored financial/inventory back-ups to the network. The majority of our company was back running as usual in 3-4 hours. Without the off-site backup we would have been in a really tough position.

The data we lost on our shared network folders was 80% older files which was kind of like having your storage unit destroyed that had been accumulating junk for 10+ years. You lose some valuable items but also a lot of junk that made it hard to find what was important anyway!

In process security measures:

We are in the process of creating a dedicated network for our VOIP phones (outside the firewall) and have a policy change to NEVER create a user without immediately creating a password and have also set-up a VPN to connect offsite to remote desktops. We perform updates on systems and anti-virus regularly on all computers and we are formalizing our communication on IT issues with users. Finally, we now have offsite back-ups of all shared folders on a nightly basis.

Lessons Learned

I've found in my life that learning from others' mistakes is a lot less painful then making the mistakes yourself. That is why I'm here today, to encourage you to help small businesses learn from my, and others, experiences to avoid going through it with their company.

There's a saying that "what we learn most from history is that we learn very little from history," let's try anyway by looking at a WWII example that works quite well as an example of the psychology behind the relaxed approach many small businesses have taken in relation to cyber-security:

In the years running up to the beginning of the second world war the British government was extremely concerned that in the event of hostilities breaking out, the German Luftwaffe would launch significant

attacks against Britain and especially London. With an estimated 250,000 casualties in the first week alone, the consensus was that millions of Londoners would flee, leaving the industrial war engine to grind to a halt. Several psychiatric hospitals were even set up on the outskirts of London to handle the huge numbers of casualties psychologically affected by the bombing.
History shows us that the psychological results expected never materialized, despite horrific numbers of casualties and extensive damage to homes, property and businesses throughout London.

A Canadian psychiatrist, J. T. MacCurdy, in his book *The Structure of Morale* postulated this was because the effect of a bomb falling on a population splits them into three groups:

1. The people killed by the bomb. As MacCurdy puts it, "the morale of the community depends on the reaction of the survivors, so from that point of view, the killed do not matter." Put this way the fact is obvious, corpses do not run about spreading panic.

Harsh, but true in this model.

2. The Near Misses. The ones that feel the blast, see the destruction but survive, deeply impressed. It may result in 'shock' and a preoccupation with the horrors witnessed.

3. The Remote Misses. These are the people who hear the sirens and the explosions, watch the aircraft overhead, but the bombs explode down the street. For them the experience of the bombing is that they survived easily, unlike the Near Miss group. The emotional result of the attack is a feeling of excitement with a flavor of invulnerability.

Near miss = trauma, remote miss = invulnerability.

Diaries and recollections of the period certainly support these theories. For instance, when a laborer was asked if he wanted to be evacuated to the countryside (after being bombed out of his house twice) he replied; "What, and miss all this? Not for all the tea in China!"

The reason for this attitude, the sense of invulnerability, is that they have been through the very worst of time - and survived. They had faced their fears, and realized they were not as bad as they thought they were going to be, and, in fact, the result of surviving had given them a sense of elation that made them feel even more alive than before.

On the subject at hand we can categorize all small business owners into these three categories: Those that have been hacked but didn't survive (direct hits). Those that have been hacked and survived (near misses), and those that have never been hacked (remote misses, - unhacked, by luck or precaution).

Now it probably goes without saying why the 1st category, those that get hacked and don't survive, aren't likely to be going around advertising it and probably have enough trauma from the event to produce a strong desire to forget it ever happened. They are also likely embarrassed by what happened and would prefer to keep it to themselves. This category of small business owner, we'll call them "Hacked to death," are probably busy starting a new business or working for someone else, leaving them with little free time to talk about what they are trying to forget anyway.

The second category is likely more prepared then many of those in the first and, unless it happened quite recently, have probably set up a very secure computer system at their companies that are safely backed up behind a hardware firewall….. or have abandoned using computers altogether in favor of pencil and paper along with their trusty fax machines, these business owners sporting their flip phones and calculators are willing to give up the productivity of computers for the safety of the tried and true - not likely a recipe for long term success.

The last category is the "remote miss" group. They've heard about companies being hacked on the news but nothing has hit anyone close enough to get their attention. They probably believe they are too small to be a target, have sufficient security in place or are just unlikely to be attacked. This group is who we are most likely trying to get information to, but like the Londoners of WWII there is a feeling of invulnerability that comes from hearing about what has happened to others that hasn't happened to them. Let's face it, if many of the largest companies on the planet along with some of the most sophisticated countries can get hacked so can they. Granted they are big targets and small business might not be but the cyber criminals are starting to realize that small, vulnerable, easy targets can be very lucrative.

For small businesses that are part of the lucky group that haven't yet been attacked or compromised this is a great time to realize the fact that they aren't immune to cybercrime, attacks are becoming more likely and frequent, not less, and the threat isn't going to go away so now is a great time to focus on understanding, analyzing and investing in the necessary precautions to keep themselves protected.

Recommendations:

Knowing the psychology of those that have not yet been directly impacted by cybercrime is useful in formulating a strategy to help them. They need to be informed that they are a target and that increasingly small businesses are being successfully attacked. Spreading the word about this reality is critical to getting their attention. Once they are convinced there is a significant threat they need to be educated on how to protect themselves. You already have great resources available to small businesses and I would recommend finding ways to actively spread the word and further leverage them.

The Idaho SBDC helped our business write its initial business plan, obtain its initial funding and weather the storms of growing a small business over the last 18 years numerous times through coaching and classes. I now sit on the advisory board of the Idaho SBDC. I see how the SBDC has started responding already. The SBDC already has good resources in place to help prevent or mitigate the devastating effects of cyberattacks including a vulnerability assessment and other tools. They also run a listserve that shares best practices with other SBDCs nationwide. However, SBDC need to be empowered to fully develop these resources and help actively promote them to small business. These resources need to be not just further developed but actively promoted to the small business community. This could be done through public service type announcements that could be sent through various social media platforms targeting small businesses. Federal agencies also need to be encouraged to collaborate with SBDCs and promote them as a resource. There are nearly 1,000 SBDC locations, the SBDCs are the "boots on the ground" coaches across the country who can educate those at risk and help those dealing with a cyber-attack on their business.

I would also recommend encouraging cybersecurity training programs and developing common resources for SBDCs to use to aid and inform small business. The Department of Homeland Security and the other federal agencies have a lot of resources and knowledge but that knowledge is hard for small businesses to find and use. I am encouraged that SBDCs and those agencies are already working on this effort due to language this committee supported in the 2017 Defense bill.

There is also a need to establish standardized, reputable certifications for cybersecurity professionals along with a way for small businesses to confirm the credentials of cybersecurity providers. When dealing with I.T. issues many small business owners are wary since it is hard to know what exactly the people you hire are doing and it is difficult to know if they should be trusted with your information.

This results in businesses often choosing not to do anything since it is both costly and seemingly risky to hire someone. Thankfully, SBDCs are already involved with the IT community to identify qualified providers but more remains to be done.

I hope that my testimony will help make a difference in combatting cyberattacks and it has been an honor speaking with you today.

Chairman RISCH. Thank you, Ben. I appreciate it. And now, Ms.—am I pronouncing it right, "Youbate"?

Ms. ABATE. Abate.

Chairman RISCH. Abate. My staff is really good about doing phonetics. I am just not good at reading phonetics.

Ms. ABATE. That is okay.

Chairman RISCH. Welcome. We would like to hear your testimony.

STATEMENT OF GINA Y. ABATE, PRESIDENT AND CEO, EDWARDS PERFORMANCE SOLUTIONS, ELKRIDGE, MD

Ms. ABATE. Okay. Well, thank you, Chairman Risch, Ranking Member Cardin, and members of the Committee for the opportunity to testify.

The high risk of financial damages is an unprecedented challenge to small businesses, intensified by the fact that the vast majority are unprepared to properly protect their assets. Discussions with hundreds of small businesses by the Cyber Security Association of Maryland members demonstrates a clear pattern of inaction, with the most frequent explanations being, "My business is small. I am not a target," "Cybersecurity is expensive and I cannot afford it," and "I am not a regulated business so I do not need to worry about it."

Let us address these justifications. Attackers are targeting small businesses with increasing frequency and sophistication. If an attacker is able to compromise a business system, they can access that to exploit business data, attack business customers and suppliers, and may even shut down the business. For an attacker, any foothold is a good foothold.

So what should a small business do to start their cybersecurity program? Every business should invest the time to understand the value of their assets, engage experts to understand the vulnerability of their IT systems, and take appropriate steps to manage their cyber risks. The more valuable their assets and the weaker their ability to detect, stop, and mitigate cyber damages, the greater the risk.

The absence of regulation should not be a driver for a cybersecurity program. In fact, regulatory compliance should be an outcome of a well-structured security program, not the reason for it. Small businesses who adopt a framework, like the NIST Cybersecurity Framework, are able to implement a cybersecurity and risk program to address current regulations and those that earn the future.

Cybersecurity is a continuous process, not a one-time event, and best approached using proven methods. Small businesses must implement a culture of safety, leveraging employee situational training, and low-cost tactics, like enforcing proper passwords, encrypting hard drives, and limiting user ability to load undesirable software.

The concepts of the NIST Framework are straightforward, but, in practice, organizations become overwhelmed with the information. It is important to note that organizations do not need to address all cybersecurity concerns at once. In most cases, a prioritized approach is sufficient to ensure key systems and/or business units are protected before addressing secondary areas of concern.

Even with the best protection tools and procedures in place, cybersecurity risk is not eliminated, so continuous monitoring is required to quickly detect malicious, undesirable, or abnormal activity. Once a breach is detected, an immediate response is critical. Businesses must have an exercised and maintained plan in place during "peace time" to ensure business damage is minimized, with the necessary actions and resources established to regain their client trust.

It is imperative the small business community understands cybersecurity is critical to overall business success. It is not just an IT problem. The challenge lies in convincing small business of the urgency to do more in protecting their assets. The compromise of one business can often impact suppliers and customers. There is much more at stake than the failure of one business at a time.

But how do we incentivize small businesses to start preparing? In Maryland, the bipartisan Cybersecurity Incentive Tax Credit Bill, Senate Bill 228, made Maryland the first State to incentivize small businesses to purchase local cybersecurity protections and investors to advance Maryland's cybersecurity companies.

Those of us at CAMI are especially excited because thousands of small Maryland businesses at risk of cybersecurity damages can now get the help they need at a lower cost. I believe it will be an indicator if this type of program generates increased conversations between cyber solution providers, both products and services, and motivates small businesses to take action.

So thank you again for the opportunity to testify, and I look forward to discussing this topic further.

[The prepared statement of Ms. Abate follows:]

EDWARDS
PERFORMANCE SOLUTIONS

Testimony before the U.S. Senate Committee on Small Business and Entrepreneurship

Gina Abate
President and CEO, Edwards Performance Solutions

Preparing Small Businesses for Cybersecurity Success

Thank you Chairman Risch, ranking member Cardin, and members of the committee for the opportunity to testify today. I am Gina Abate, President and CEO of Edwards Performance Solutions, a Woman Owned Small Business, as well as the Chair of the Board for the Cybersecurity Association of Maryland, Inc. (CAMI).

The high risk of financial damages is an unprecedented challenge to small businesses, intensified by the fact that the vast majority are unprepared to properly protect their assets. Discussions with hundreds of small businesses by CAMI members demonstrate a clear pattern of inaction, with the most frequent explanations being:

- "My business is small, I'm not a target."
- "Cybersecurity is expensive and I can't afford it."
- "I'm not a regulated business, so I don't need to worry about it."

Let's address these justifications. Attackers are targeting small businesses with increasing frequency and sophistication. If an attacker is able to compromise a business system, they can use that access to exploit business information, attack business customers and suppliers, and may even shut down business operations entirely. For an attacker, any foothold is a good foothold.

So, what should a small business do to start their cybersecurity program?

Every business should invest the time to understand the value of their assets, engage experts to understand the vulnerability of their IT systems, and take appropriate steps to manage their cyber risk. The more valuable their assets and the weaker their ability to detect, stop, and mitigate cyber damages, the greater the risk.

The absence of regulation should not be the driver for a cybersecurity program. In fact, regulatory compliance should be an outcome of a well-structured security program, not the reason for it. Small businesses who adopt a framework, like the NIST Cybersecurity Framework, are able to implement a cybersecurity and risk program to address current regulations, as well as any new regulations, with minor program changes.

Cybersecurity is a continuous process, not a one-time event and best approached using proven methods. I recommend the NIST Cybersecurity Framework in conjunction with the guidance of expert cybersecurity practitioners. Small businesses must implement a culture of safety – leveraging employee situational training and low-cost tactics like enforcing proper passwords, encrypting hard drives, and limiting user ability to load undesirable software.

The concepts of the NIST Cybersecurity Framework are straight forward, but in practice, organizations become overwhelmed with information. It is important to note that organizations do not need to address all cybersecurity concerns at once. In most cases, a prioritized approach is

sufficient to ensure key systems and/or business units are protected before addressing secondary areas of concern.

Even with the best protection tools and procedures in place, cybersecurity risk is not eliminated. Continuous monitoring is required to quickly detect malicious, undesirable, or abnormal activity. Once a breach is detected, an immediate response is critical. Businesses must have an exercised and maintained plan in place during "peace time" to ensure business damage is minimized, with the necessary actions and resources established to regain client trust.

It is imperative the small business community understands cybersecurity is critical to overall business success. The challenge lies in convincing small businesses of the urgency to do more in protecting their assets. The compromise of one business can often impact suppliers and customers; there is much more at stake than the failure of one business at a time.

But, how do we incentivize small businesses to start preparing? In Maryland, the bi-partisan Cybersecurity Incentive Tax Credits Bill (SB228) made Maryland the first state to incentivize small businesses to purchase local cybersecurity protections and investors to advance Maryland cybersecurity companies. Those of us at CAMI are especially excited because thousands of small Maryland businesses at risk of cyber damages can now get the help they need at lower cost.

Thank you again for the opportunity to testify. I look forward to discussing this topic with you further.

Gina Abate – Bio

Gina Abate is the President and CEO of Edwards Performance Solutions (Edwards), a Woman Owned Small Business (WOSB) helping organizations achieve secure operational performance. Gina's strong leadership and industry knowledge enables strategic plan development for growth and to advance the company's mission. Under her leadership, Edwards expanded its offerings to include cybersecurity and IT services, complementing a strong enterprise management and training history.

Ms. Abate is also the Board of Directors Chairperson for The Cybersecurity Association of Maryland, Inc. (CAMI). She is featured in multiple publications promoting cyber awareness and was recently recognized by The Daily Record as one of their "Most Influential Marylanders" for her contributions to current and emerging technology.

Prior to joining Edwards, Ms. Abate was a Vice President at NTT Data Federal Systems (formerly Keane Federal Systems) and BAE Systems. She has 30+ years of proven leadership with executive, technical, and business management experience in the Federal Government as a Civil Servant and a commercial sector contractor.

Chairman RISCH. Thank you so much. We are going to do a round of questions now, and I will start with myself.

Ben, do you have any objection to telling us a little bit about the ransomware attack that you survived? I guess you survived.

Mr. TOEWS. Yeah, I would be happy to share whatever I can.

Chairman RISCH. Do it.

Mr. TOEWS. Just like what more information would you like?

Chairman RISCH. Well, I do not think anyone here has any information about it, so maybe you could give us a brief description of what happened and how you got through it.

Mr. TOEWS. Yeah. So, I mean, we, on a Friday, we essentially set up a new user, and after we set up that new user, that did not have a password and was plugged into the network, and then over the weekend, from what we can tell, they got into our system. We had ports open, because we have a voice-over-IP system, which is difficult to have it behind the firewall. And so that opened up ports for them to get into our system. We figured they probably used, I think it is called a brute force hacker system, that allows you to get—figure out who does not have a password, which users do not have a password. And then once they were in our system, they just encrypted all of the shared network files, including all of our operations and inventory and financial information. And fortunately, like I said, that was backed up.

Chairman RISCH. And so what—was that the end of it? I mean, did you wind up having to do some—I mean, obviously you had to go in and change the system.

Mr. TOEWS. Yeah. We restored our system. On Monday morning, we figured it out. We had the ransom note in there. We did not pay any money. I think it was in bitcoin that they tried to get us to pay. We did not pay any money to restore our files. We just thought it was too risky. You know, what are the chances that the criminals are going to actually give you the information that they are promising you?

And so we restored what we could, that had been backed up offsite, and once we restored that we were back up and running pretty quickly, and we just, honestly, lost some labor hours for specialized reports that were on our network. But all of our customer information was stored offsite, so there was not any sensitive information that was breached.

Chairman RISCH. Sounds like you were pretty lucky getting through it.

Mr. TOEWS. We were very lucky. Yes, I would say so.

Chairman RISCH. Senator Cardin.

Senator CARDIN. Well, I thank all of our witnesses. I want to drill down a little bit on what the SBA can do to help. The 2017 National Defense Authorization Act included language that this Committee had reported out, that required the SBA and the Department of Homeland Security to collaborate on cyber strategies for small businesses, using the Small Business Development Centers.

Mr. Schrader, you have already talked about some of the work with the Small Business Centers, or maybe Mr. Toews. One of you had talked about the use of those centers.

The bill also required the two agencies to report back to our two authorizing committees with a strategy on how they are going to deal with cybersecurity. That report should have been in by the end of 2017. It has not yet been received, and our staffs are following up to do that.

My question is, what can you expect could be helpful from the Small Business Administration, to help small businesses deal with being better prepared on cybersecurity? I think, Mr. Schrader, you talked a little bit about the private sector, having their conferences. That is great. I do not know how many small businesses actually take advantage of that. But there is already contact between a lot of small businesses and the SBA. Could they be more effective in getting greater knowledge to the small businesses and how they need to go about in order to understand their risk factors and take common sense ways of protecting themselves?

Mr. SCHRADER. That is a terrific question, Senator, and, absolutely, yes. There are so many small businesses out there, small- to medium-sized businesses, as part of the supply chain, as well as entrepreneurial standalone access that know public partnership, or private entities such as NCSA can reach all of them. We need to have a lot of different things, people working in the same direction. There is so much more education that can go out there. Whether it comes from the cybersecurity education work that we are doing with Department of Homeland Security, we would happily partner with the SBA to work on some of these educational programs.

We have developed a really nice adaptation of the NIST Framework that is geared to very hands-on education. Whether we move that more online, whether we are able to access more of the centers outside of Washington in order to do more of that training, we absolutely see a wonderful partnership opportunity.

Because there are certain simple, actionable steps that will help never make one totally secure, but will make you much more secure than you are. For example, as you talked about in the ransomware, there was no password. You had just plugged it in on a Friday. The simple things, like put in a password, keep your patches up to date, make your passwords actually pass-phrases, look at two-factor authentication. Very simple steps that people just need to have put out to them in an easy way that they can remember, that it is not an IT part of business, it is a day-to-day, ongoing part of the business.

Senator CARDIN. Mr. Castro, you mentioned some common-sense ways, including the co-op. I think the co-op is an excellent suggestion. You are sort of at the mercy of the private sector on products to buy and the price factors can be astronomical for individual small business owners. So the services of a co-op seem to make a lot of sense, in first directing you to the right type of product, and secondly, getting you a competitive price. I like that.

Ms. Abate, you mentioned the fact that the Maryland legislature passed a bill that allows for credits against State income taxes in regards to locally produced cybersecurity software. It will be interesting to see how that works, because we could look at that at the national level, but I think it might be interesting to see what happens first in Maryland.

These are, it seems like, common-sense approaches that could be taken. What do you need from us in order to advance some of these proposals?

Mr. CASTRO. I think certainly SBA needs to be pointed in the right direction on some of this. They are not necessarily actively pursuing a lot of these initiatives. You know, one of the challenges, I think, is there is a lot of information that is out there on the training side, and on the education side. There is not really concentrated around what is the full curriculum, how are you either specifically educating the workers in small businesses so they know what they need to do, or how are you giving them that step-by-step guidance of walking someone through who is never going to get the training but you can show them, once, how to do the thing they need to do at that moment. And both of those are needed, and right now SBA just is not doing it.

Senator CARDIN. I just hope you would follow up on what is happening in Maryland. I find that fascinating, whether other states follow suit and what the experience is in our State.

Ms. ABATE. Yeah, I think so too, and I think part of the issue, when you look at small businesses, we have much more limited funds, correct, than a large. So what are we focused on? We are focused on how do we deliver a quality service, a quality product? How do we remain profitable? And, you know, cyber really, for a lot of these companies, has not risen to that business success, and anything we can do, through SBA or others, to help to raise it to that level—like I said, it is not just an IT problem. You can lose your business. Everything you do, all day, to be profitable and have a fabulous product is put at risk if you ignore this piece of the pie. I mean, it truly can. And I think it is just critical to raise awareness on what they need to be focused on.

Chairman RISCH. Thank you.

Senator Inhofe.

Senator INHOFE. Thank you very much, Mr. Chairman.

[Off microphone.]

I find it interesting that we have—there might be some relationship between—I think we probably have more small businesses, and some of the rural states do, than some of the larger states. I have one example in Norman, Oklahoma. We have a company called Astronomics. There is no reason that you guys should have ever heard of it, but it is a small business, and they specialize in designing certain kinds of telescope.

Anyway, they were successful when they saw justice when a California man was convicted in a Federal court of directing distributed denial of service cyber attack in Astronomics. Now, they were successful. It worked. Now, Mr. Castro, what can we do to have more successes like this? What needs to be changed that might be something that you would like to see us do?

Mr. CASTRO. Yeah. I think one of the most important things is really around that certification side, so that workers—so that small businesses can hire workers who have some skills, because I think so often, you know, the small business just has no real capacity to do anything, and they have no capacity to measure the skills. And there are so many classes that are out there right now, but there is no verification that, you know, you have taken the class and you

have actually absorbed the knowledge. I mean, I have taken a class on juggling. I cannot juggle. And that is kind of what exists right now in the cyber certification space.

Senator INHOFE. Mr. Schrader, I chaired the Environment and Public Works Committed for 12 years, and during the time of the Obama administration, and I am sure some of this Committee would disagree with this characterization. But we did just a lot of overregulation in every area, and we were successful, and this President came along and doing away with some of these regulations. As a matter of fact, there are two ways of doing away with the regulation. One is with Executive order and the other with a CRA, and our count is up to 70 now.

Now, I think that is one reason that our economy has really been booming, the overregulation, of course. I think the tax bill helped too. What types of regulatory problems do you have, because that is an area where we might be—or do you have any regulatory problems?

Mr. SCHRADER. At the NCSA we do not have regulatory problems. In fact, the NIST Framework which has been put out, and is continuing to be updated, has been very helpful in that it is voluntary and that it is scalable, and that it is something that puts out the kind of common-sense ways that the private enterprises have been able to come through and to make useful to small businesses.

In our particular case, because we have a very active Board of Directors, who is very interested in pushing out this education, we have been able to move it into small businesses, and anything that would encourage further contributions, and other further ways that we can roll out this education through private means, is something that we very much like.

For example, Senator, I actually had a very nice conversation with Devin Barrett and Dan Hillenbrand in your office about different ways that we would be able to work with the Administration and with yours on some of the very simple tools to be used, both within staffs here and staffs at Small Business, because each office really is, almost, a small business, and you have to take a look at everything that you are doing in order to make cybersecurity part of your everyday way of doing business.

The crooks are not sleeping. The people who are coming in and trying to steal our IP are not sleeping. They are constantly going after something. You cannot have something that says "I have checked that list off. Now I am done," because there are always people looking. It is an ongoing process that we always need to be watchful for.

Senator INHOFE. Okay. I was here for your opening statement. Ms. Abate—is that——

Ms. ABATE. That is it.

Senator INHOFE [continuing]. And you commented that there is something in Maryland that was, I guess, a State agency or something, that has given help, and I did not know what you were talking about.

Ms. ABATE. The Cyber Security Association of Maryland, it is called CAMI, is a nonprofit, and it supports our Maryland cybersecurity companies by helping connect them with buyers of products

and services, and then we also work to make sure we have the necessary workforce to be able to perform that work.

Senator INHOFE. Okay. That is interesting. I would like to get to know more about that. Thank you, Mr. Chairman.

Senator RUBIO [presiding]. Thank you.

Senator Heitkamp.

Senator HEITKAMP. Thank you, Mr. Chairman. This is cybersecurity day for me. I spent the morning with Assistant Secretary Jeanette Manfra over at the Department of Homeland Security, and we just came away from a hearing for Christopher Krebs to become the Under Secretary. So we are trying to gear up over at DHS.

One concern that I have, probably for all of you, is that—let me give you an example. We have a Center of Excellence in the Centers for Disease Control. They look and research various diseases. That information is utilized by all kinds of agencies, you know, whether it is the Bureau of Prisons, whether it is the Department of Human Services.

One of the things that I am very concerned about is the disparate kind of jurisdiction over cyber within the government, and I believe that Mr. Krebs has a responsibility to create a center of excellence, that then can be integrated in other agencies. But this is the best way to engage the private sector.

I also talk a lot about, you know, everybody wants a magic bullet that will harden the system and protect, and we are all looking for that software, all looking for that hardware, potentially, that is going to harden the system. Guess what? You know, that does not exist. It is not likely to exist. And what we really need is we need good cyber hygiene, and that is really what you all are talking about in small businesses is good cyber hygiene. What does that look like and where is the checklist?

There are two ways we can do that. We can have the Department of Homeland Security or whatever agency we designate to create a center of excellence for cybersecurity that people can look at best practices. I am not saying you have to use them, but create the best practices, the best tools for educating users. You know, you are only as secure as your least secure user, in terms of a back door, ask Target about that, right?

And so what do we do to create greater awareness among not just small business users but your constituents, your customers, to create better security, better cyber hygiene? And, Mr. Toews, I can assure you, coming from the University of North Dakota, I know how to pronounce your last name. And for those of you, that is a hockey joke. Wonderful, wonderful alumni of our hockey program and we are proud to—even though he is from Manitoba, and I can talk like I am from Manitoba if that will help.

Anyway—eh. I should not say "ya." I should say "eh." But help me out here on what tools you think your small businesses, or your organizations would need to better educate your users, your customers, on how to protect themselves.

I will start with you, Mr. Castro.

Mr. CASTRO. Yeah. I mean, one of the biggest challenges right now is, you know, just so much information that is on these different websites. And so I think one of the opportunities that this

Committee has is to really talk to SBA about how it is going to consolidate the information.

When I was, you know, preparing for this hearing, one of the things I tried to do was put myself in the position of if I was a small business owner today, trying to look for this information right now, I had an attack and I was trying to respond. Could I find anything? And what I was finding was that, again, first of all, the information just is really badly organized. It is not put in a user-friendly format. But also there is just so much information. So much of it is outdated. You know, it is not serving the customer.

Senator HEITKAMP. And it is cumbersome.

Mr. CASTRO. Exactly. And so, you know, really forcing SBA to confront this issue and how they are going to work with the different agencies. Clearly SBA is not going to be the center of excellence for cybersecurity, but they are the ones that are communicating it to the small businesses.

Senator HEITKAMP. Right. But I think, in some ways, they do not know.

Mr. Schrader.

Mr. SCHRADER. Yes. Well, first, thank you, Senator, for mentioning Assistant Secretary Manfra. She was kind enough to come to RSA——

Senator HEITKAMP. She told me that.

Mr. SCHRADER [continuing]. Last week, and on Thursday we had a panel together at eight in the morning, about increasing the diversity in the cybersecurity workforce, because it is very difficult to build up, you know, a very good, diverse workforce that is ready to jump in to fill the need that we have now. And then she was kind enough to come to a lunch with the directors and some others, and she gave about two hours of her time talking about what DHS is doing, and talking about the strong public-private partnership that we have.

Senator HEITKAMP. Do you agree, Mr. Schrader, that creating a center of excellence within the Department of Homeland Security, then that information being disseminated in places like SBA, could be enormously helpful?

Mr. SCHRADER. I think that everything that we can do is helpful. As you pointed out, there is no silver bullet. There is no hardened defense. It has to be layers of defense. It has to be constantly looking at different needs.

I started here talking about cybersecurity, my business, but as Assistant Secretary Manfra and I have talked about, we are also doing Lock Down Your Login, which is geared specifically to staff members here in Congress. Right now we have some posters which we will happily give out to you. But the idea is six easy tips that will help everyone here, because you are a very attractive target, for emails, your social accounts, and the rest.

Senator HEITKAMP. Not just us but every person in the United States wants to know how to fix this problem. And I am sorry, Mr. Toews and Ms. Abate, I have run out of time. But this is an issue that we are going to continue to have discussions on. But I really think it is important that we see all this jurisdictional, you know, what is DoD doing, what is DHS doing, what is SBA. Because everybody is coming at it with a sense of panic, when we need to sit

down and have a systemic kind of—like I said, the center of excellence that then can disseminate information and get it to the local community organizations that can do seminars with, you know, at AARP, or in high schools, saying this is what you need to do to not be—to lock the door.

Thank you, Mr. Chairman, for the extra time.

Chairman RISCH [presiding]. Thank you. Senator Rubio.

Senator RUBIO. Thank you, and the thing that concerns me—well, let me share a story with you about a company, a small company in Florida. They got hacked. Somebody got—criminals got into their system, basically stole all of their client data and information, took it all, and then basically contacted them and said, "We know how much you can afford to pay. We have your financial information. You need to pay us. You need to pay us in bitcoin if you want all this back, or you will not be able to operate."

And they went to the FBI, according to them—I have not talked to the FBI about this case—and the FBI basically told them, "You should pay them because you are not going to get your data back if you do not." And so they did. They went out and bought, I think it was a quarter of a million dollars of bitcoin and paid them, and they got their information back, and were able to continue to operate. So they had their financials, they knew what they had in the bank and what they could afford to pay, and they based their demands on it. We will never knew who stole their money, but it is gone, and it was damaging to that company, as you can well imagine.

Now if that had been someone—if we had a rash of people breaking into companies and stealing cash out of safes, you know, we would be all talking about it. In this particular case, they probably did not even want to publicize it, which is why I do not say who the business is, because their clients are probably concerned about it. We do not have a lot to do to help them, and their bigger challenges in the future—they have gotten a little better at what they are doing but they cannot afford to have the sort of IT division to protect them again in the future.

And is the story I have just outlined, do you think, number one, just from the experience you have all had, is this happening more than we know? In essence, are businesses experiencing this but basically not filing a quote-unquote "police report" the way they would a normal theft because (a) there is nothing law enforcement can to do to help them, and (b) it is not the kind of thing they want people to know about? Do you think this is—do you think it is common and under-reported?

Ms. ABATE. I do. I think more and more small businesses do not want to talk about it because it does damage their reputation and it can have a really adverse effect. But, you know, the other thing is reaching out to the right law enforcement and what you need to do and having processes.

This morning I was at a session. The Secret Service was there. Unbeknownst to me, they can assist and help, and we were talking about that earlier.

So I think it is really important for companies to understand, when you do experience a breach, who can I reach out to and what are the best next steps? Because if they do not have a plan in

place, you are in panic mode, right? I mean, your business is at risk. You have lost your data if you do not have substantial backup.

So it is something, I think, that is a problem and needs to be addressed.

Mr. TOEWS. I echo that. I think it is very under-reported. We never contacted law enforcement at all in our situation. Of course, we recovered most of the information. But we are unique in the sense that we did not have—all of our customer databases were offsite, so I am comfortable talking with you about it.

But I think you are right. I think people are embarrassed and they are concerned it will have a negative impact on their business, and so they just do not talk about it. So it is an under-reported issue, but it has got to be impacting our economy. I know it is.

Senator RUBIO. And the follow-up, the other thing that is devastating about it is if that business happens to do work for governments, or health care, some of the information that is being stolen is proprietary health care records, billing records, the like, and in the case of government, contracts, whether it is DoD or the space industry that is trying to expand to bring in more small businesses and suppliers, the inability to meet certain criteria for cybersecurity, because of the governmental—forget about classified. Just the governmental component of it could potentially begin to disqualify smaller companies because they cannot afford to build up the cyber capability necessary to be able to service the client.

And so is that also something that people are running into in the small business world, where the cost of building up the sort of IT security they need is too high and, therefore, prohibit them from certain types of work that might now, or in the future, have certain minimum IT strength requirements that they cannot afford to purchase?

Mr. CASTRO. I will comment first. I mean, it is a challenge, I think, right now for any small business to comply with all the different Federal security regulations at the same level the agencies are expected to require, and I think agencies are struggling at the same—with the same issue. I think it is feasible to put together a cybersecurity plan. The problem is most small businesses do not have the capability.

Senator RUBIO. They cannot afford it.

Mr. CASTRO. They cannot afford it and they do not have the, I think, even skill set to start putting it together.

Ms. ABATE. You know, I would just mention that we have actually had customers, when we have worked with them on an assessment, and looked at what needed to be done, have decided not to do work with the DoD because of the expense in complying with the 800–171. It is just not something they can justify when they weigh it.

Senator RUBIO. And I guess this is just a statement, and I think you guys would agree with this. If we are serious about expanding more government contracting work to small businesses, because we want to have a broader base of suppliers, then part of that program needs to be assisting companies with the costs—small companies with the costs of, and the capability of being able to meet the criteria that we require of them. In earnest, trying to attract more

suppliers and small business providers to do work in the space industry or for defense, the only way that is going to happen is if we help them to meet some of these criteria that on their own they cannot afford.

Mr. SCHRADER. Right. Some of the larger companies are, in fact, realizing that that is a problem because they realize that they have problems in the supply chain and in their vendor management, and they are looking at public and private ways to do it. For example, Federal Express came to us and made a contribution to us in order to do the cybersecurity business program. And they asked to have one of their trainings done in Memphis, where they have a lot of small business contractors, and also asked to do one in Charlotte, where they also have a significant presence.

So they were very proactive. They were very good corporate citizens in realizing that they were getting a two-fer. One is they were helping small businesses be safer themselves and be able to compete with larger ones, but at the same time they were protecting their own business model because they would be able to do business with a supply chain with a better degree of assurance that they were dealing with people who took cybersecurity as seriously as they did.

Chairman RISCH. I am shocked to hear that the private sector is ahead of the Federal Government on some of this, as we all are.

Thank you, Senator Rubio.

Senator Markey.

Senator MARKEY. Thank you so much. You know, this is a problem that is not small, because we see big companies constantly being hacked. And when I ask Joe Tucci, who is the CEO of EMC—they own RSA, which is kind of a standard for the entire industry, RSA—I say, "Why are all these companies getting hacked, the big companies?" and they say, "Well, they do not want to buy our state-of-the-art security." It is a never-ending, always escalating technology versus technology, spy versus spy. Like Mad magazine, it just never ends. You just have to keep investing if you want to be protected.

So if big companies do not like to do it, and then they get hacked, how hard is it for small companies, and, really, that is why this hearing is important today, because it is not—IoT is the Internet of Things but it is also IoT, Internet of Threats, because everything is going to be a threat, going down the line, because everything is going to be ultimately digitized. And we could have as many as 50 billion IoT devices, in our pockets, our homes, our businesses, by 2020, 50 billion of these devices in the United States.

And so there is just going to be a vast proliferation of the ability to hack in. And we have, as you know, up in Massachusetts, my little travelogue, we have scores of cybersecurity companies now. You know, RSA is kind of a famous one but we have scores of these companies. We buy Israel's companies. Israel buys our cyber companies, because it is, for better or worse, an incredibly huge growth industry, and it is because our prosperity, our privacy, our Nation's security is all dependent upon us moving more surely into this area.

And it is certainly threatens small businesses in our country, which is why I introduced the Cyber Shield Act. And so just listen

to what the bill would do if it became the law. It would establish an advisory committee of cybersecurity experts from academia, industry, consumer advocacy communities, and the public to create cybersecurity benchmarks for IoT devices. And it can be baby monitors, cameras, cell phones, laptops, tablets, anything that you are using in any of your businesses.

And the IoT manufacturers can then voluntarily certify that their product meets those industry-leading cybersecurity and data security benchmarks and display that certification to the public. So that would then reward the companies that are making the technologies that you want to be sure are not going to get hacked in your small business, that are going to give you the protections which you want. But in the same way when you buy a car, you can see the safety sticker. Is it one through five stars? You can look at lighting, one through five stars. You can look at it in so many other aspects of our lives.

Well, cybersecurity, increasingly, is going to have to be in that case because you have to purchase the equipment, the devices that are going to make you prosperous as small businesses. So it would reward the manufacturers by adhering to the best data security practices while also ensuring that small businesses can make more informed choices.

So my question for the panel is, do you think that creating cybersecurity certification regime, such as the Cyber Shield Act does for IoT devices, is helpful for small businesses when they are making purchasing decisions?

Mr. CASTRO. I think it is a really important move to try and get the market to work better, because I think what your bill will do is it creates that transparency in the market which is sorely lacking right now. I think it is a great move. I think you might be able to do it with a little bit less of a certification regime if you maybe just required IoT vendors to disclose their security practice without assessing it. Let a third party assess it. But whether it is this advisory committee that assesses it or a third party, I think it is exactly what we need to get that kind of market transparency to work.

Senator MARKEY. And can you talk about that flying blind quality to the marketplace, you know, if you are a small business or anyone else?

Mr. CASTRO. Yeah. I mean, the biggest problem for a small business is they do not know who the best of the best is, right? Sometimes they go based on a brand name that they have heard, but often, you know, I used to work, you know, directly with small businesses and you go in and they were using some product they had never heard of, because, you know, their, you know, cousin recommended it, and that cousin did not know anything about security. Or, you know, they had a popup on a website tell them, you know, they had an antivirus and they better click here and download it, and they thought they were improving security and they were not.

Senator MARKEY. Right. So that is a problem, right? I mean, if a big company cannot figure it out, or they are just too cheap and they do not want to spend every couple of years, the updated, you know, software money, then they get hacked and everyone says

"what happened?" and then, you know, my biggest company says they did not want to pay us, you know, for the security. It is tougher for you. It is harder for you to have the money, you know, to be doing that on an ongoing basis, but at least the transparency of which one of these technologies has been given a one- through five-star rating, at least you have got some idea as to what the level of security which you have purchased for any one of these devices might be.

So is it Mr. Toews—is that how you say it? Why is it "Taves"? It is T-o-e-w-s. What country is that?

Chairman RISCH. You missed Heidi Heitkamp this morning.

Senator MARKEY. Oh, did I? Oh, my God.

Chairman RISCH. Very interesting.

Senator MARKEY. Yeah. But what country?

Mr. TOEWS. Germany.

Senator MARKEY. Germany.

Mr. TOEWS. So the W makes a V sound——

Senator MARKEY. Yeah.

Mr. TOEWS [continuing]. And O and E is trying to imitate——

Senator MARKEY. Got it.

Mr. TOEWS [continuing]. A vowel we do not have.

Senator MARKEY. So, see, great minds think alike. Like Heidi, I do not want to know the answer.

So we are actually at the beginning of the ransomware epidemic, where cyber criminals infect their victims' computer networks with malware, denying users access to their files until a ransom is paid. And that ransomware attack could prevent a hospital from accessing its patients' medical records, a business from accessing their financial records, a police department from accessing files from ongoing investigations. And attackers have even taken aim at municipalities, like the town of Medfield, Massachusetts, which was forced to pay a $300 ransom to hackers who attacked their municipal network. And that cyber threat to anyone who connects to the internet is clear, and we need to take decisive action to deal with that.

So, Mr. Toews, can you talk about what kind of protections you would like to see in order to be protected against ransomware extortion?

Mr. TOEWS. Certainly. I would be happy to. And it is a very uncomfortable situation when you find all of your files encrypted and there is a ransom note. It is not something that you expect to happen. But I honestly think that one of the first steps we need to take is to educate small businesses more that it is a problem. I do not believe that most of them understand the gravity of the problem. They all feel like this could not happen to me.

So somehow educating them, getting, like I said, a public service announcement, some way of getting the word out, maybe let them know how many companies have been hacked, maybe letting them know how many of those that we know got hacked, how many it ended in the business going out of business. That kind of information going to the small businesses, I think, would be key. And then certifying—having standardized certifications that show who reputable cybersecurity professionals are, I think would be a huge

step. Maybe there are already some out there. It needs to be educated—we need to be educated on that as well.

Senator MARKEY. Yeah. We have a company up in Massachusetts called Carbonite. Carbonite had almost no employees eight years ago and now it has 1,200 employees. So they have already dealt with ransomware for 10,000 companies in America. In other words, if you have one call to make, and it just happened 20 minutes ago, and you do not call Carbonite, you are probably making a mistake. Okay?

That is my travelogue here, because they can fix it maybe within an hour, if you make the call on the right day, immediately, right? Because this is just an epidemic across the country, and you do not want to have to pay that ransom. You want to have to be able to figure this thing out immediately where it is in its earliest stages.

So that is also another problem for smaller companies. You know, it is now going to become increasingly an additional expenditure which has to be made, you know, in order to deal with this as it just proliferates, because there is, ultimately—you know, there is a Dickensian quality to the internet. It is the best of wires and the worst of wire simultaneously. It can enable, it can ennoble, it can degrade, it can debase. And this sinister side of cyber space is increasingly, in industry, a bad—the bad guys, right?

So that is why we are here, and we are looking forward to any recommendations you can give to us. But I do think, ultimately, we need some national standards that we just start to establish, at least information, transparency, so that the information is in the hands of the small businesses, so they are making informed consumer choices for their small businesses, to protect their company against ransomware or against any other attacks.

So thank you for your testimony. I thank you, Mr. Chairman. This is a very, very important hearing.

Chairman RISCH. Thank you. Senator Markey, your idea about the standards in your legislation, does it contemplate an entity like UL, Underwriters Laboratories, that would somehow put their seal on——

Senator MARKEY. Ah.

Chairman RISCH. UL was successful for generations, of course. And I would ask the panel, would—does a cyber product lend itself to that kind of a certification like they would have for UL, when it comes to security, or is that something you need to think about?

Mr. CASTRO. Some products I think it does make sense, especially when you are talking about devices. Others, you know, when it is more service-based, you know, you might look at other types of certifications like TRUSTe and others that have existed. So I do not think it is always a straightforward answer.

The biggest difference is that with UL there was a straightforward testing. With cybersecurity, the testing that you can do to identify flaws is much harder. It is a bigger open space.

Chairman RISCH. We had a witness in—I do not think this is classified—it was in the Intel Committee, and we were having a cybersecurity hearing. And this person, who was an expert on cyber stuff said, "We are in cyber where the Wright Brothers were on their second airplane," saying that, you know, the biggest problem

is we do not know what we do not know. And I suspect maybe we are going to be crossing those bridges.

Senator MARKEY. But there are—if I may, Mr.—there are companies like Carbonite. There are, really, RSA, which is a subdivision now of Dell, which has purchased EMC, which now has RSA in it. If you go to the state-of-the-art company, they are fierce competitors against the Russians, or against any other, you know, criminal——

Chairman RISCH. The problem——

Senator MARKEY [continuing]. But you have to pay for it in order to get it done, and they can actually attract the most talented people in the government to go and work for them, because they can pay so much more.

Chairman RISCH. The problem is, is the average buyer, consumer, does not know that stuff. I know some pretty sophisticated people that have gone out and bought Kaspersky Laboratory products. Anybody ever heard of them?

Senator MARKEY. Yeah. Can I say this? Woburn, Massachusetts, yeah. I am just being a Ben Cardin.

Chairman RISCH. Thank you very much.

Senator MARKEY. Yeah. But that is not, maybe, the best example for us to be advertising.

Senator CARDIN. I think this is very important, your bill. There is some work being done at NIST in regards to this field, but I do not think we have what you are trying to do, Senator Markey. But it is something we need to be able to get better conformity.

And what you have indicated, about not reporting this, is common. Rarely is this reported, which points out another problem, because if we are trying to counter this and we do not get that information to some law enforcement investigative authority, then it makes it even more challenging for us to root out those that should be held criminally accountable for the type of activities that they are doing.

So I think you are pointing out some real significant issues, and all of you have come up with proposals, which we thank. I mean, that is what I like from hearings, specific proposals. So I think you have given us a lot of really good ideas.

Senator MARKEY. And if I may, I think your UL idea is a good idea. It is a good way of thinking about it.

Chairman RISCH. It is a good way of thinking about it. I do not know if it works or not.

Senator Cantwell.

Senator MARKEY. Yeah, but I can I just say to Mr. Castro——

Chairman RISCH. Senator Markey has been taking up all your time.

Senator MARKEY. I have been filibustering so you had time to get here, okay? That has been my responsibility.

I just want to say to you, Mr. Castro, given what happened in Cuba last week and how responsible we will be to you, you are the most powerful Castro in the world now, so let us know what you think.

Chairman RISCH. Moving right along, Senator Cantwell.

Senator CANTWELL. Well, Thank you, Mr. Chairman, and thank you for having this hearing. It is such an important hearing be-

cause we want our small businesses to be able to keep pace with the level of advancements, and certainly with the level of attacks on our infrastructure as it relates to cyber attacks, we want our small businesses to have every opportunity.

I know my colleague was here earlier talking about cyber hygiene, and one thing we have been able to do in the Pacific Northwest is working with our industry sectors, actually and our Guard and Reserve has come up with that cyber hygiene list of things that we expect all businesses to do.

What would it take for—what do you think we should be specifically focusing on that would help small businesses participate in those kinds of discussions and to better reveal information about what kinds of attacks you might have already been experiencing, given that nobody really wants to come forward and say that, because of vulnerabilities to your business?

Chairman RISCH. Well, who is the hero here?

Mr. CASTRO. I will start it. I think, you know, a lot of small businesses do not have a lot of time to spend on this issue, so, you know, you always have to, when we are talking about how can we help them, is giving them very concrete, actionable steps.

The New York Times did something great recently, where they had a seven-day financial health program. Every day you signed up for it you got an email that said, you know, spend an hour and do these specific things. You know, look at your credit card statements. Use this tool to figure out what you are overpaying for. That is the kind of direct, hands-on feedback we need to give small businesses.

The average small business is not going to be able to do—you know, they are not going to be able to sit down and think about the cybersecurity threats and, you know, take a tip about, you know, secure your passwords, and think through all the ways that could apply. They need very concrete direction that says, you know, log into your Wi-Fi router and make sure you have been labeled WPA security. That kind of specific feedback. And I think, you know, we can do that, but that is not what we have been doing so far.

Senator CANTWELL. Okay.

Mr. SCHRADER. The other part is it has to be ongoing, right, because with UL you have a UL sticker on your lamp. You plug the lamp in and you know that the lamp is going to be safe when you plug it in. But in the case of small businesses, they are constantly adding, they are upgrading, there are patches to be fixed, there are new ways that they are bringing in new software, new hardware, which is the issue that you had, Ben.

And so basically you have to have a recency effect as well as an education effect. It has to be something that they constantly think of as they go through their day-to-day business, keeping their software up to date, changing their passwords when they change their—you know, their employees, being a little bit of a socially aware of the kind of social engineering that happens to big and small firms, in order to get people to, you know, to download things or to reveal passwords.

So it is an ongoing education process. It is not like we will ever be able to say, "We have hit the bottom of the list. Thank you very

much. That is solved. Let us move on." And we do not want that to be, because we want to encourage more entrepreneurship. We want to encourage them to be able to compete into the supply chain and to grow into bigger companies.

Senator CANTWELL. It is amazing that Equifax was just—there was an available patch, you know, an Apache patch that somebody just did not download. Like somebody made a really big mistake by not implementing that solution. So I hear your point about constant information.

That is why—I do not know if it is because we had so many people in our Guard and Reserve that were in the software industry or just that we have a big footprint there, but this effort on a cyber hygiene list, I just feel—I mean, look. I mean, now the threat is not necessarily somebody sticking a sub in U.S. waters or basically flying a plane into U.S. airspace. It is state-owned actors hacking systems.

So I actually think the Guard and Reserve could play this ongoing dialogue for us about what are the 10 things people should be on the lookout for? What are the 10 cyber hygiene things that could be deployed? But anyway, they are doing that in our State, and it is a good partnership with industry.

Mr. SCHRADER. That is interesting, because a partnership that the National Cyber Security Alliance has with DHS, in October we sponsor Cyber Security Awareness Month, where it is a constant drum on different aspects of how we will go and get the word out on different things, and we will do follow-ups in different areas, Data Privacy Day, and then some other.

We are doing, right now, something called Spring Clean Your Machine. Just as, you know, my grandma used to push around the sofas and pull down the curtains and open up all the windows and spring-clean the whole place. Do that with your machine. Delete the apps that you do not use. Upgrade your pass phrases. Figure out who is looking at your location data. The little simple things and reminders that are helpful along the way.

Senator CANTWELL. Great. Thank you, Mr. Chairman.

Chairman RISCH. Okay. Thank you very much. Ben, have you got anything more for the good of the order?

Senator CARDIN. Just to thank our witnesses and to point out the challenges we have. You could do everything right and you still can get attacked. Supply chain issues, so many different things going on. So we have to have a greater understanding and knowledge in the small business community so they can take reasonable steps, and we need to figure out best strategy.

Chairman RISCH. Thank you very much. Thank you all for spending your time with us. I think this has been one of the more productive hearings I have been in, in quite a while. It has given us a lot to think about. Some of the suggestions that have been made here, we will do our best to try to implement.

What I am going to do is I am going to keep the record open until 5:00 on Friday. If any of you have anything more for the record, please feel free to submit. Any members who want to submit questions for the record, we will do it that way.

So with that, thank you again. This hearing is adjourned.

[Whereupon, at 4:51 p.m., the Committee was adjourned.]

APPENDIX MATERIAL SUBMITTED

Senate Committee on Small Business and Entrepreneurship Hearing
April 25, 2018
Follow-Up Questions for the Record

Questions for Mr. Daniel Castro

Questions from:

Senator Young

In your testimony, you cite a recent survey that found that only 12 percent of small businesses reported having developed a cybersecurity response plan and only 21 percent reported providing security awareness training to employees.

QUESTION 1:

What does an effective cybersecurity response plan look like for a small business?

A cybersecurity response plan provides an overall plan for how an organization should respond to a cybersecurity incident. It identifies the roles and responsibilities of different stakeholders and specific procedures to follow.

QUESTION 2:

Can you summarize the key components of such a plan?

A cybersecurity response plan should address all key steps in responding to a cybersecurity incident, including preparation, detection, containment, investigation, remediation, and recovery. Preparation involves identifying key assets and preparing strategies to protect and manage those assets. Detection involves monitoring various systems for threat analysis and incidents. Containment is the initial triage stage once an incident is discovered, to limit the impact of an incident and ensure evidence is retained and the necessary parties are notified. Investigation involves determining the cause of the incident and its impact. Remediation is used to repair systems that have been compromised. Finally, recovery is used to incorporate lessons learned into future planning.

QUESTION 3:

Can you speak to what that role would look like – specifically, what steps should the federal government take to play an effective, collaborative role in small business cybersecurity prevention efforts?

As mentioned in my testimony, there are three concrete steps the federal government can take to improve small business cybersecurity prevention efforts. First, the federal government can

establish a certification program for "part-time" cybersecurity professionals. Too few qualified cybersecurity workers are currently available, and there is not a useful cybersecurity credential option for workers who have cybersecurity responsibilities but do not have this as their primary job responsibility. Second, the federal government should create a cybersecurity boot camp for small businesses. This program would enable any business to create a basic cybersecurity program and take steps to prevent common vulnerabilities. The federal government provides some cybersecurity resources and training to small businesses, but they could be substantially improved and consolidated. Moreover, outdated material should be removed from government websites. Third, the federal government can help form a small business cybersecurity co-op to create a large pool of willing buyers for various cybersecurity products and services, including cyber risk insurance.

QUESTION 4:

Would a government certification – a "government seal" – be an effective approach? Take the U.S. Green Building Council's LEED certification for environmentally friendly buildings – would this sort of certification be helpful?

There are various attempts to certify products as secure. More information can reduce market asymmetries and lead to better outcomes, especially among less sophisticated buyers. A "government seal" (or government-endorsed private sector seal) could be effective provided that the costs and process of receiving certification were not prohibitive.

Questions from:

Senator Heitkamp

Mr. Castro, in your testimony, you noted that one-third of businesses were not taking pro-active steps to protect against cyber threats, half of businesses were not allocating any budget for risk mitigation services, and only 12 percent of businesses had developed a cybersecurity response plan. Convincing small businesses that they are legitimate targets for cyber-attacks is absolutely essential to motivating them take cybersecurity seriously.

QUESTION 1:

In your view, how should the federal government go about persuading small businesses, especially those who have not yet been impacted by cybercrime, to take cybersecurity seriously?

Small businesses can only make good decisions about cybersecurity if they have good information about threats and how to mitigate those threats. The federal government can provide information about known risks and emerging risks to small businesses. It could consider creating a cybersecurity liaison within the Small Business Administration to more actively engaging with the small businesses community, such as by speaking at industry conferences and events about the impact of cybercrime on small businesses. The federal government can also provide information about best practices and encourage a small business co-op that can evaluate

cybersecurity products for small businesses. The federal government can also publicly release its own assessment of various cybersecurity products.

During the hearing, you noted that websites that provide information on cybersecurity can be poorly organized and not user-friendly, and you said the Committee could consider discussing with the U.S. Small Business Administration (SBA) the importance of consolidating the information in a way that makes it easier for businesses to find and disseminate the information they need.

QUESTION 2:

Could you briefly elaborate on how the current structure of websites make it difficult for individuals to find and attain the information they need? What should agencies like the SBA keep in mind when organizing and posting cybersecurity information online?

There are at least three problems. First, there is too much poor-quality information available from government agencies. For example, some of the information on these government sites is outdated and other information lacks sufficient detail to be useful. Second, there is not enough high-quality information on emerging threats and best practices. Small businesses need to receive concrete, actionable steps on how to address security threats, not well-known platitudes. Finally, the information on these sites is often poorly organized and duplicative. Multiple government agencies attempt to provide the same or similar cybersecurity information to small businesses. This creates confusion for users and makes it harder to find useful information quickly.

The SBA should coordinate and collaborate with other government agencies to ensure the federal government speaks with one voice on providing cybersecurity information to small businesses. Moreover, it should conduct usability testing for its websites and use human-centered design to prepare and evaluate its online cybersecurity awareness and training materials.

Questions from:

Senator Hirono

I have heard from numerous business owners in my state who are interested in expanding their businesses online, which, for companies in Hawaii, can really make a difference as they look to expand to mainland markets and beyond. As part of supporting these businesses in their efforts to expand, I have worked to convene local businesses with different online companies over the last several months.

QUESTION 1:

While understanding that many small businesses lack the same resources as larger businesses to invest in cybersecurity protections, what reasonable changes can small business owners make to protect themselves and their brands as they look to expand online?

There are a number of key cyber risks for businesses as they expand online, such as new threats to online systems and data, and key challenges such as implementing strong authentication mechanisms. However, every small business is different, so each will have to evaluate its own set of cyber threats and tolerance for risk. This should include identify key assets and the steps necessary to protect them; evaluating internal capabilities and limitations; and developing a plan for responding to cyber incidents. One good resource for this process is the NIST Cybersecurity Framework.

QUESTION 2:

In your view, what pro-active steps can they take to ensure they are protected against cybersecurity threats?

At a minimum, these small businesses should create a basic cybersecurity program, and a process for regularly evaluating and improving it. Achieving good cybersecurity is like eating well or exercising—it is not something that can just be done once, rather it is about improving an organization over time.

Vice President, Information Technology and Innovation Foundation (ITIF)

Mr. Castro, in your testimony, you highlight that while many small businesses are concerned about cybersecurity attacks, which cost the U.S. economy between $57 billion and $109 billion in 2016, most have not taken pro-active steps to protect themselves from attacks. You elaborate that resources at the Small Business Administration (SBA) and elsewhere have been limited, and could be updated or improved. Given that small businesses generally face the same kinds of cybersecurity threats as larger businesses, but lack similar resources to protect against cyberattacks, you have recommended that SBA establish a "Cybersecurity Boot Camp" to help small business owners better identify, detect, and respond to cybersecurity incidents.

QUESTION 3:

Can you briefly elaborate on how these "boot camps" could benefit small businesses by providing them with the practical information they need?

To take the exercise analogy from above, the purpose of fitness boot camps is to teach new skills, train hard to get immediate results, and establish new long-term routines. Similarly, a cybersecurity boot camp would be designed to allow small businesses to improve their cybersecurity through short-term, focused training sessions that result in both immediate improvements to their baseline security and create long-term changes in the organization's cybersecurity routines. For example, participants in cybersecurity boot camps would be given a set of specific tasks to complete and guidance on how to complete them. The complexity of the tasks (and level of success in completing them) will depend on the experience of the participant, and those who repeat boot camps will gain additional results. Tasks could change based on

emerging threats, such as checking for the need for specific patches and applying them, to more routine activities, such as checking security system logs, to basics, such as establishing a password policy for an organization.

QUESTION 4:

Furthermore, in your view, how could SBA leverage its relationships with its federal government partners to promote its cybersecurity resources?

Many other federal government agencies will likely have more cybersecurity expertise than the SBA. However, the SBA has the strongest relationship with the small business community, and it can serve as a conduit for information to this community. It can also ensure that the rest of the federal government understands the specific needs and threats facing small businesses.

Question from:

Senator Duckworth

QUESTION 1:

Small businesses are prime targets for cyber-attacks yet often lack the resources necessary to invest in a robust cybersecurity infrastructure and maintain strong, updated and secure information systems. What specific policies would you recommend Congress consider in trying to promote a new status quo, where every small business considers effective cyber security policies to be a core competency alongside sound accounting, marketing and human resources practices?

The recommendation to establish a certification for workers in small businesses who are responsible for cybersecurity but do not have this as their primary job function would go a long way to changing the norm in these businesses. If this certification were available, small business owners would be able to determine whether they have someone on staff with proper training to implement a security program. And by retaining someone on staff with this training, small businesses would begin to incorporate cybersecurity planning into their decision making.

Senate Committee on Small Business and Entrepreneurship Hearing
April 25, 2018
Follow-Up Questions for the Record

Questions for Mr. Russell Schrader

Question from:

Senator Young

QUESTION 1:

How can I work with you and stakeholders in my state to bring your successful cybersecurity workshop to Hoosier small businesses back home?

- The National Cyber Security Alliance is happy to engage in discussions to bring our successful CyberSecure My Business program to Indiana. You can reach out to our Director of Small Business Programs, Daniel Eliot, to begin that process. His email address is: daniel@staysafeonline.org.

Questions from:

Senator Heitkamp

Mr. Schrader, I appreciate the partnership between the National Cyber Security Alliance (NCSA) and the Department of Homeland Security to educate the public on the importance of adopting good cyber-hygiene practices. Increasing the public understanding of the steps they need to take to navigate the web safely and securely is an essential ingredient to keeping them protected against cyber threats.

QUESTION 1:

In your view, how effective has the STOP. THINK. CONNECT. campaign been in educating the public on cyber-hygiene. Are there aspects of the program that you believe could be enhanced? Is there a role Congress should play in supporting your efforts?

- NCSA believes that the STOP. THINK. CONNECT. campaign has been very effective in generating awareness about online safety. In addition to National Cyber Security Awareness Month (October) and Data Privacy Day (Jan. 28), NCSA initiates a variety of integrated, timely campaigns around seasonal news hooks (i.e., Digital Spring Cleaning) to keep online safety "in the news" in a user-friendly context. NCSA has generated strong and extremely positive results, with STOP. THINK. CONNECT. messaging as a cornerstone in both traditional and social media.

- NCSA and the U.S. Department of Homeland Security believe that STOP. THINK. CONNECT. is due for a refresh. Today, everyone is "connected" and the messaging

needs to be updated to reflect certain behaviors like shopping, banking and social media. For example, the updated campaign could spotlight the following: "STOP. THINK. SHOP.", "STOP. THINK. BANK." and "STOP. THINK. POST."

- Congress could certainly assist in supporting NCSA's ongoing efforts by sharing various campaign messages and materials at the state and local level – particularly during National Cyber Security Awareness Month and Data Privacy Day.

I also appreciate your testimony regarding the NCSA's CyberSecure My Business program, which offers a series of workshops based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework to educate small and medium sized businesses on how they can be safer and more secure online.

QUESTION 2:

To date, to what extent have the workshops enjoyed participation from a diverse group of businesses (i.e. businesses in every sector, businesses in both rural and urban areas, etc.)?

- The majority of participation in our webinars and workshops are small to medium sized businesses with fewer than 100 employees, government entities, and non-profit organizations. We have also engaged businesses from all sectors in our workshops (restaurants, child care, retail, manufacturing, etc.). This is large part due to the partnerships we create when we go into each state--particularly each district's Small Business Administration, Better Business Bureau, trade associations, and local chambers. We target a mix of urban and rural areas. For instance, in February, 2018 we held a workshop in Memphis, TN. In March, 2018, we held a workshop in the Village of Silver Lake, OH--a rural community outside of Akron.

QUESTION 3:

Given the potential value that this program provides businesses, do you anticipate the program expanding or providing additional workshops in the future?

- Because of the positive feedback we are getting from attendees, community partners, and program sponsors, NCSA does plan to grow the program to provide additional workshops and resources in the future. Much of that, however, is dependent upon financial sponsorship to enable us to grow it.

Questions from:

Senator Hirono

I have heard from numerous business owners in my state who are interested in expanding their businesses online, which, for companies in Hawaii, can really make a difference as they look to expand to mainland markets and beyond. As part of supporting these businesses in their efforts to

expand, I have worked to convene local businesses with different online companies over the last several months.

QUESTION 1:

While understanding that many small businesses lack the same resources as larger businesses to invest in cybersecurity protections, what reasonable changes can small business owners make to protect themselves and their brands as they look to expand online?

Below are a few reasonable changes businesses can take:

- Protect accounts with strong authentication. Enable multi-factor authentication and have strong passphrases to make it more difficult for hackers to gain access to systems.
- Keep software current: Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats. A reasonable change could be to automate this process so the small business does not forget to update. This also includes mobile devices.
- Back up data: Put in place a system – either in the cloud or via separate hard drive storage – that makes electronic copies of the key information on a regular basis. This process can also be automated. The more the small business can automate, the easier it will be for them to manage.
- Use encryption software to protect customers' financial information from theft during transactions. This is sometimes confusing for small businesses, and some prefer to outsource this to a third party if they are unsure how to do this themselves.
- Limit access to data or systems only to those who require it to perform the core duties of their jobs. When they limit access to data, they limit exposure.
- Connect to the internet safely: 1) make sure they are accessing their critical data using a secure network--not public wifi and 2) if they offer customers free wifi, make sure that is not the same network they are using to access their business data.

QUESTION 2:

In your view, what proactive steps can they take to ensure they are protected against cybersecurity threats?

- The first step in protecting a business from cyber threats is to identify the "crown jewels" of your business – those assets and systems that are critical to your business. Crown jewels are the data without which your business would have difficulty operating and/or the information that could be a high-value target for cybercriminals. Create a detailed inventory list of data and physical assets and update it routinely. Record the manufacturer, make, model, serial number, and support information for hardware and software. For software, know the specific version that is installed and running.

- Build a culture of cybersecurity that includes employees knowing how to protect themselves and the business and understanding the cyber risks as your business grows or adds new technologies or functions.
- Keep security software current: Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.
- Back up data: Put in place a system – either in the cloud or via separate hard drive storage – that makes electronic copies of the key information on a regular basis.
- Limit access to data or systems only to those who require it to perform the core duties of their jobs.
- Keep a clean machine: Companies should have clear rules for what employees can install and keep on their work computers.
- Email. Look for unusual requests, attachments, links. Be suspicious.
- Having a recovery plan created before an attack occurs is critical. Make and practice an incident response plan to contain an attack or incident and maintain business operations in the short term.
- visit: https://staysafeonline.org/cybersecure-business/ for links to each phase of the NIST framework and tools that help implement each one.

QUESTION 3:

Mr. Schrader, in your testimony, you describe NCSA's programs and workshops, which take place every year to help small businesses improve their cybersecurity posture. While understanding that it may be difficult to hold conferences and host events in locations like Hawaii given its relative distance from the U.S. mainland, what kinds of outreach efforts has NCSA made to promote its online resources for companies in Hawaii and companies elsewhere that are similarly situated?

- NCSA hosts monthly webinars, the second Tuesday of every month from 2-3pm EDT, that are attended by small businesses from across the globe to ensure we are reaching as many SMB's as possible outside of our in-person workshops.
- NCSA welcomes opportunities to engage in specific training opportunities with constituents of Hawaii and companies situated in similar locations.

Mr. Schrader, in your testimony, you also describe the partnership between the Department of Homeland Security (DHS) and your Board of Directors, which includes industry stakeholders across the technology, financial, insurance, hospitality, and telecommunications sectors. You discuss how this partnership allows you to provide educational resources to support federal, state, and local governments, local businesses and business organizations, and related stakeholders in identifying, detecting, and responding to cybersecurity threats.

QUESTION 4:

Can you briefly elaborate on the kinds of resources you provide these stakeholders, and describe the trainings that are most beneficial for them?

- NCSA has developed a workbook based off the NIST Cybersecurity Framework. This workbook accompanies our in-person workshop and enables the SMB to begin to create a written information security plan. It also provides them a wealth of resources to assist them in this endeavor. 100% of workshop attendees have said that after the workshop they continued to work on the workbook or that they plan to.
- Our monthly webinars cover a vast array of topics, including securing email to training employees, to evaluating vendor security. These webinars are recorded and stored on our website, www.staysafeonline.org. Attendance has regularly ranged from 400 to 1000 attendees.
- NCSA also allows industry and federal partners to author or co-author blogs, infographics, etc. and house them on our website for small businesses and other stakeholders to access.
- NCSA also has created a CyberSecure My Business newsletter, which goes out monthly highlighting our upcoming trainings, partner events.

QUESTION 5:

NCSA trainings support federal, state, and local leaders. Can you describe the trainings that are most useful for government officials?

- NCSA's Lock Down Your Login program is designed to educate government staff on basic cyber hygiene. We work with congressional staff members on a monthly basis to educate them on the 6 principles of Lock Down Your Login.
- NCSA also regularly has government officials attend our CyberSecure My Business workshops, as government agencies operate much like a business and can benefit from all of the lessons taught in the workshop.
- NCSA welcomes more opportunities to engage with government officials at the federal, state and local levels.

QUESTION 6:

NCSA trainings also support businesses and business organizations. Can you describe the trainings that are most useful for local businesses, Chambers of Commerce, and Better Business Bureaus?

- The CyberSecure My Business in-person workshops and related webinars are recognized as useful by Chambers of Commerce, Better Business Bureaus and local small businesses due to our unique approach, blending federal, private and non-profit partners and delivering the material in a non-technical and empowering way.

Mr. Schrader, in your testimony you allude to NCSA's ability to leverage the experience of its members, including those who represent the hospitality sector. Given the importance of the tourism industry in Hawaii and the variety of businesses tourism supports both directly and indirectly, the hospitality sector is extremely important for businesses in my state.

QUESTION 7:

Have you worked directly with small businesses within the hospitality sector, and, if so, then can you briefly describe any particular challenges these kinds of businesses may encounter?

- We target our marketing materials to all industries and have had individuals from the hospitality sector attend our workshops and web-based trainings.
- A few particular challenges the hospitality sector experiences are: Protecting Point of Sale systems and door lock systems and training and retraining a workforce that has high turnover.

QUESTION 8:

Can you describe the trainings and resources that are most useful for businesses that rely on tourism?

- The general cybersecurity tips NCSA provides transcends all industries. However, NCSA is able to go work with trade organizations to go into more depth and customize our CyberSecure My Business program to any industry, including tourism. For instance, NCSA worked with Ford Motor Company and CDK Global to customize the CyberSecure My Business program for automotive dealers. NCSA welcomes opportunities to work with governments and trade organizations to develop materials for specific industries.

Questions from:

Senator Duckworth

QUESTION 1:

Small businesses are prime targets for cyber-attacks yet often lack the resources necessary to invest in a robust cybersecurity infrastructure and maintain strong, updated and secure information systems. What specific policies would you recommend Congress consider in trying to promote a new status quo, where every small business considers effective cyber security policies to be a core competency alongside sound accounting, marketing and human resources practices?

- NCSA, a nonpartisan educational nonprofit, encourages policies that provide the small businesses community with easy-to-access and low-cost/free training, materials, and subject matter experts that facilitate improved security.
- NCSA also supports a unified, inter-agency source of guidance from government regarding small business cybersecurity awareness and resources.

QUESTION 2:

You testified that the National Cyber Security Alliance uses the National Institute of Standards and Technology (NIST) framework when advising small businesses. How accessible do you find the framework to be for small businesses and what can we do to tailor the NIST framework for different audiences? Are there any other public frameworks or guidance you use to help guide small businesses as they approach cybersecurity?

- NCSA has found the NIST Cybersecurity Framework to be quite accessible to the SMB community, and the "Profiles" documents NIST plans to deliver soon will only make the Framework more accessible.
- Small business cybersecurity materials from DHS C3 and the Federal Trade Commission's Consumer and Business Education are public guidance NCSA regularly uses to help guide small businesses as they approach cybersecurity.
- As NCSA engages with various industries, the sources of guidance vary. However, another widely accepted source of guidance is the Payment Card Industry Security Standards.

Senate Committee on Small Business and Entrepreneurship Hearing
April 25, 2018
Follow-Up Questions for the Record

Questions for Mr. Ben Toews

Questions from:

Senator Heitkamp

Mr. Toews, I appreciate you sharing with the Committee your recent experience in responding to and recovering from a ransomware attack. Your story highlights the critical importance of having multiple lines of defense, regularly updating systems and programs, and continually backing up important information in a separate physical location. In your testimony, you noted the importance of convincing small businesses that they are not immune to cybercrime.

QUESTION 1:

In your view, how should the federal government go about persuading small businesses, especially those who have not yet been impacted by cybercrime, to take cybersecurity seriously?

I believe that sharing the current reality of the increasing number of small businesses that are attacked along with the devastating consequences to those that are not prepared would be very helpful. Until we experienced the attack, and consequently became involved with the SBDC's efforts to inform small businesses about the threat, I had no idea how many small businesses are impacted. Some sort of public service announcement with the facts and statistics would be eye-opening. Leveraging the SBDC as a great resource for informing businesses about the threat and educating them how to protect themselves would have a great impact since they are already working with small businesses all around the country.

QUESTION 2:

Are there existing programs or efforts underway that you believe are effective in demonstrating the threats posed to small businesses?

The SBDC has a cybersecurity toolkit on their website(s) which incorporates an assessment tool for small businesses to determine how prepared they are for an attack along with the resources to be prepared and protected. I believe the resources are already available but just need to be leveraged by finding ways to get the word out. Further classes to the small business community from the SBDC would also be helpful to educate utilizing the existing small business coaches.

QUESTION 3:

Does there need to be an increased focus on motivating businesses to take action?

Yes, the idea of a tax credit for cybersecurity costs was suggested at the hearing and may be an effective way to lower barriers for smaller businesses to invest in cybersecurity. Again, just finding a way, via social media for instance, of informing small businesses of the high rate of attack and potential damage would be a great motivator.

Questions from:

Senator Hirono

I have heard from numerous business owners in my state who are interested in expanding their businesses online, which, for companies in Hawaii, can really make a difference as they look to expand to mainland markets and beyond. As part of supporting these businesses in their efforts to expand, I have worked to convene local businesses with different online companies over the last several months.

QUESTION 1:

While understanding that many small businesses lack the same resources as larger businesses to invest in cybersecurity protections, what reasonable changes can small business owners make to protect themselves and their brands as they look to expand online?

First, let me say that I am reading your question while vacationing on Waikiki Beach and have to say that your state has to be one of the most beautiful places on earth! This is my family's first visit but won't be our last.

The least expensive measure that can make a significant difference is simply training users how to spot and avoid the various forms of attack along with best practices for username and password management. Posting guidelines for users and reviewing them even monthly can go a long way in reducing risk of successful attack. The information is free on SBDC websites and the only cost is taking the time to go over the information. The cost of offsite back-ups (cloud storage) is very low with unlimited storage available at less than $100/year in the current market. With little investment a small business can have ways to prevent attacks and restore information.

QUESTION 2:

In your view, what pro-active steps can they take to ensure they are protected against cybersecurity threats?

Utilizing the SBDC cybersecurity assessment is a great way to find areas of vulnerability and determine action items to address them. The assessment actually works as an educational tool because as you answer the questions about your company you have a realization of what it takes to keep you secure.

Question from:

Senator Duckworth

QUESTION 1:

Small businesses are prime targets for cyber-attacks yet often lack the resources necessary to invest in a robust cybersecurity infrastructure and maintain strong, updated and secure information systems. What specific policies would you recommend Congress consider in trying to promote a new status quo, where every small business considers effective cyber security policies to be a core competency alongside sound accounting, marketing and human resources practices?

One idea is to create federal minimum security standards for software products that contain private or financial information stored in their databases. For instance QuickBooks, probably the most common financial software used by small businesses, requires that you disable certain server security features for full functionality. This could also be accomplished by a non-profit who provided a seal of approval for software that meets these standards.

Another idea that was mentioned during the hearing was a cybersecurity tax credit where small businesses would get a credit for investing in cybersecurity.

Senate Committee on Small Business and Entrepreneurship Hearing
April 25, 2018
Follow-Up Questions for the Record

Questions for Ms. Gina Y. Abate

Questions from:

Senator Young

QUESTION 1:

Can you speak to what that role would look like – specifically, what steps should the federal government take to play an effective, collaborative role in small business cybersecurity prevention efforts?

We read this question: *"What can Congress do collaboratively with small businesses to prevent cybersecurity breaches?"*

We believe Chairman Risch's bill, S. 2735, the Small Business Advanced Cybersecurity Enhancements Act of 2018, provides a focused start by directing the Small Business Administration in coordination with the Department of Commerce to create a central small business cybersecurity assistance unit and small business cybersecurity assistance units in each small business development center.

The units shall serve as the primary interface for small business concerns to receive and share cyber threat indicators and defensive measures with the federal government.

This bill further authorizes the Department of Homeland Security (DHS) to work with a consortium, including the National Cybersecurity Preparedness Consortium, to support efforts to address cybersecurity risks and incidents, including threats or acts of terrorism.

The bill should be amended from a 'may' to a 'shall' directing DHS to work with such a consortium to assist its national cybersecurity and communications integration center to:

- Provide training to state and local first responders and officials, develop curriculums, and provide technical assistance
- Conduct cross-sector cybersecurity training and simulation exercises for state and local governments, critical infrastructure owners/operators, and private industry
- Help states and communities develop cybersecurity information sharing programs
- Incorporate cybersecurity risk, incident prevention, and response planning into existing state and local emergency plans and continuity of operations plans

We also commend the bi-partisan approach in S. 770 introduced by Senator Brian Schatz and Cosponsored by Chairman Risch, the Main Street Cybersecurity Act of 2017.

This bill requires the National Institute of Standards and Technology (NIST) to consider small businesses when it facilitates and supports the development of voluntary, consensus-based, industry-led guidelines and procedures to cost-effectively reduce cyber risks to critical infrastructure.

NIST must disseminate, and publish on its website, standard and method resources that small business may use voluntarily to help reduce their cybersecurity risks. The resources must be: (1) technology-neutral, (2) based on international standards to the extent possible, (3) able to vary with the nature and size of the implementing small business and the sensitivity of the data collected or stored on the information systems, and (4) consistent with the national cybersecurity awareness and education program under the Cybersecurity Enhancement Act of 2014. Other federal agencies that NIST considers appropriate must also publish the resources on their own websites.

We further commend the bi-partisan approach in H.R 2184, authored by Congressman Mike McCaul and Senator Tim Kaine's companion bill, S. 754, the Cyber Scholarship Opportunities Act of 2017. This bill amends the Cybersecurity Enhancement Act of 2014 to require the federal cyber scholarship-for-service program that the National Science Foundation (NSF) coordinates with the Department of Homeland Security to include scholarship recipients who are students pursuing an associate's degree in a cybersecurity field without the intent of transferring to a bachelor's degree program and who either have a bachelor's degree already or are veterans of the Armed Forces.

In addition, the Federal Government and Congress should work collaboratively with comparable state agencies and small business associations and entities like the Cybersecurity Association of Maryland, Inc. (CAMI) to protect property, software and vulnerable transactions and provide some incentives for large businesses to engage or procure a certain percentage of services and solutions from small cybersecurity companies.

QUESTION 2:

Would a government certification – a government seal if you will – be an effective approach? Take the U.S. Green Building Council's LEED certification for environmentally friendly buildings – would this sort of certification be helpful?

A qualified yes. If the evaluation and certification scale is structured so only organizations meeting the government requirements are listed publically, this approach is likely to help influence and encourage other businesses to become cyber secure. If there is a public-facing scale, it may expose companies who are not yet cyber secure and potentially increase their vulnerability to a cybersecurity attack.

The criteria should also concentrate on the most urgently needed security measures, considering the vast difference between organizations with several employees versus those with 50-100+.

Questions from:

Senator Heitkamp

Ms. Abate, in your testimony, you noted that passage of Maryland's Cybersecurity Incentive Tax Credits bill made the state the first to incentivize small businesses to purchase local cybersecurity protections.

QUESTION 1:

Could you briefly elaborate on how this effort will get small businesses to invest in cybersecurity?

Businesses of all sizes are vulnerable to cybersecurity attacks, but small businesses are often the least equipped. Focused mainly on their day-to-day operations and with smaller profit margins than larger companies, small companies are more likely to purchase cyber solutions when incentivized. Maryland Senate Bill 228, Cybersecurity Incentive Tax Credits, provides a tax credit for up to 50% of cyber product and service costs, up to a maximum of $50,000.

The tax credit will be administered on a first come basis until the allocation of credits reach $2 million in 2018 and $4 million in 2019 and beyond. Of the allocated amounts, 25% is authorized to qualified buyers of cybersecurity services.

QUESTION 2:

Do you believe that other states should take a similar approach?

A qualified yes. Maryland is uniquely positioned as home to Ft. Meade, the United States Cyber Command, and the National Security Agency. The proximity to these organizations attracts and retains a large pool of cyber talent – making the tax incentive approach a win-win for both Maryland's small businesses looking to become cyber secure and the cyber companies looking to sell their solutions.

A modified approach should be considered in states with far fewer cyber companies. To receive competitive pricing, a more practical tactic may include a credit applicable on the purchase of cyber services or products from any state. Alternatively, states with fewer cyber companies may also benefit from this approach by growing their current market or incentivizing new cyber companies to enter the state and leverage the tax credit.

QUESTION 3:

On the national level, are there incentives Congress should consider providing to small businesses to make the necessary investments in cybersecurity?

Congress could motivate small businesses through tax incentives for purchasing cyber solutions or cyber insurance and tax credits for hiring those with cybersecurity degrees, especially for organizations with critical mission directives, such as protecting defense, the electrical grid, financial institutions, and telecommunications.

There should also be fair, equitable, and measurable merchant liability for preventable data breaches.

Questions from:

Senator Hirono

I have heard from numerous business owners in my state who are interested in expanding their businesses online, which, for companies in Hawaii, can really make a difference as they look to expand to mainland markets and beyond. As part of supporting these businesses in their efforts to expand, I have worked to convene local businesses with different online companies over the last several months.

QUESTION 1:

While understanding that many small businesses lack the same resources as larger businesses to invest in cybersecurity protections, what reasonable changes can small business owners make to protect themselves and their brands as they look to expand online?

Large or small, businesses of all sizes should create a workplace culture of cybersecurity. Establishing the security culture does not require spending a lot of money – start with an educational awareness campaign for employees and contractors on the risks, cyber threats, and attacks associated with conducting business online. Other low-cost tactics include enforcing proper passwords (selection/strength), encrypting hard drives, and limiting user ability to load undesirable software.

Small businesses may also hire business-savvy security experts, leveraging professional cybersecurity service organizations to create and implement processes and procedures – protecting business assets through policy, education, and training.

QUESTION 2:

In your view, what pro-active steps can they take to ensure they are protected against cybersecurity threats?

Businesses should begin by understanding their business objectives, organizational goals, informational assets, and how they are protected. Performing vulnerability scans of the IT infrastructure, where information assets are located, followed by regular penetration testing exercises, allows organizations to assess their overall business risk profile. Known business risks are then the starting point for building an organizational Cybersecurity Program, based on a solid framework, like the NIST Cybersecurity Framework.

President and CEO, Edwards Performance Solutions

Ms. Abate, in your testimony, you elaborate on the importance of cybersecurity for small businesses, even though many small business owners believe that they are too small to be targeted or that cybersecurity is too expensive for them to afford. You also describe how small businesses can make relatively minor changes to protect themselves from cybersecurity threats.

QUESTION 3:

Can you describe your own experience with making your business more cyber secure? What resources or incentives were most helpful?

At Edwards Performance Solutions we found creating a program based on the NIST Cybersecurity Framework (NIST CSF) is key – protecting customers' information is vital to their and our success.

Internally, we strive to provide a secure employee operating environment and create a culture of cybersecurity. In additional to regular communication and implementing multi-factor authentication (MFA), we leverage low-cost tactics like enforcing proper password strength, encrypting hard drives, and limiting user ability to load undesirable software. But, there is always room for improvement. We have defined a plan to continuously mature our program, aligned to the NIST CSF, using our in-house expertise.

QUESTION 4:

Can you describe how businesses like yours have used the National Institute of Standards and Technology's Cybersecurity Framework (NIST Cybersecurity Framework) to make themselves more secure?

While the NIST Cybersecurity Framework (NIST CSF) is not technically a maturity model, it does provide an excellent structure for defining one. We are employing the NIST CSF to structure our internal cybersecurity program – measuring our maturity and defining our strategic program investments, based on our goals, against the defined maturity model.

Ms. Abate, in balancing the limited resources of many small businesses with their responsibility to protect their customers' information, it certainly seems like the federal government could play an increased role in promoting cybersecurity.

QUESTION 5:

How significant is the cybersecurity vulnerability facing small businesses, and do the kind of cyber-attacks you see in the field require a change in tactics at the federal level?

The cybersecurity threats facing all businesses is growing and is ever evolving. Regardless of size, if a company is conducting business using modern technology, they are vulnerable to cyber threats or attacks. Businesses should look to create a culture of security and a Cybersecurity Program, beginning with awareness and training.

And, yes, I do see where attacks require a change in tactics at the federal level. Any avenues that facilitate discussion of the challenges faced in the small business community and/or increase education and communication, are beneficial. In Maryland the recent tax credit legislation has generated increased conversation and focus within the state; a win for cyber companies and those businesses unaware of their cyber risks.

QUESTION 6:

In your recommendation that small businesses look to the NIST Cybersecurity Framework in conjunction with additional guidance from cybersecurity consultants, you argue that this will help to ensure that small businesses promote a culture of safety. I'm interested to know how heavy of a financial burden it is to hire cybersecurity consultants. How many billable hours are required to audit and secure one of your small business clients in accordance with the NIST Cybersecurity Framework, and at what total cost?

Every organization is different, but the level of investment in a Cybersecurity Program must be balanced with business goals and objectives. If implemented appropriately, a Cybersecurity Program is a business asset and facilitates overall business improvement.

A quick assessment of a small business could require as little as a few days to provide valuable advice, guidance, and direction. How much it requires to bring them in line with the NIST Cybersecurity Framework is heavily reliant on their current operational state and the existing prevalent business culture.

QUESTION 7:

Are your small business clients affected by vulnerabilities in networking and security products? Would they benefit from an increased focus on security engineering on the part of these vendors?

Businesses of all sizes are subject to vulnerabilities in the products they use. Product manufacturers need to institute and/or improve their security engineering processes to

better support user needs. However, even the best engineered security product may still fail if errors or mistakes are made by the end user during configuration.

A critical part of an organizations' security program is vulnerability and configuration management. Businesses should take precautions and understand the risks associated with the systems they install and the ways in which they are configured.

Ms. Abate, in your testimony, you refer to cybersecurity tax credits, which have incentivized small businesses in your state to purchase cybersecurity protections—the first program of its kind nationwide.

QUESTION 8:

Can you briefly explain how these tax credits have worked for small businesses Maryland?

Maryland had an investor tax credit on the books to incentivize investment in cyber companies, but in 2018, the Maryland General Assembly passed legislation on Senate Bill 228 – Cybersecurity Incentive Tax Credits. The tax credit legislation provides a tax credit for up to 50% of cyber product and service costs, up to a maximum of $50,000. The tax credit will be administered on a first come basis until the allocation of credits reach $2 million in 2018 and $4 million in 2019 and beyond.

The bill was signed into law by Governor Larry Hogan on May 15, 2018 and becomes effective July 1, 2018.

QUESTION 9:

How have they encouraged businesses to invest in cybersecurity protections?

The Cybersecurity Association of Maryland (CAMI) believes with the proper marketing and outreach, this tax credit, much like Maryland's bio-tech tax credit, will reach capacity quickly once the application process opens. While there is a monetary tax credit cap of $2 million in 2018 and $4 million in 2019 and beyond, CAMI anticipates a sufficient need and desire to increase these monetary amounts legislatively in years to come.

Questions from:

Senator Duckworth

QUESTION 1:

Small businesses are prime targets for cyber-attacks yet often lack the resources necessary to invest in a robust cybersecurity infrastructure and maintain strong, updated and secure information systems. What specific policies would you recommend Congress consider in trying to promote a new status quo, where every small business considers effective cyber security policies to be a core competency alongside sound accounting, marketing and human resources practices?

We agree cybersecurity should be the status quo, in addition to a core competency for businesses of all sizes, new and old. Implementation would be best served by a phase-in approach – creating grants or tax credits for businesses with critical mission directives, such as protecting defense, the electrical grid, financial institutions, and telecommunications. Congress may also consider a requirement or guidelines that small businesses, who wish to do business with the Federal, State, or municipal governments, demonstrate a certain degree of cybersecurity protection.

Additionally, a 'new status quo' should begin at the federal level. Congress should ensure that it has appropriate authority to countermand Executive Orders that may allow foreign companies to access our technology and promote greater potential breaches of our cybersecurity systems, such as recently announced trade agreement with China's telcom, ZTE.

QUESTION 2:

What types of cybersecurity investments and what information security best practices should new small business owners prioritize when starting a company with limited resources?

Large or small, businesses of all sizes should create a workplace culture of cybersecurity. Establishing the security culture does not require spending a lot of money – start with an educational awareness campaign for employees and contractors on the risks, cyber threats, and attacks associated with conducting business online. Other low-cost tactics include enforcing proper passwords (selection/strength), encrypting hard drives, and limiting user ability to load undesirable software.

Small businesses may also hire business-savvy security experts, leveraging professional cybersecurity service organizations to create and implement processes and procedures – protecting business assets through policy, education, and training.

Statement for the record of

C. E. "Tee" Rowe
President/CEO
America's SBDCs

Hearing on
Cybersecurity

Committee on Small Business
and Entrepreneurship

United States Senate

April 25, 2018

Chairman Risch, Ranking Member Cardin, members of the committee. Thank you for allowing me to submit this statement on behalf of America's SBDC, the Association of Small Business Development Centers.

SBDCs operate over 1,000 centers in all fifty states as well as the District of Columbia, Puerto Rico, the Virgin Islands, American Samoa and Guam. SBDCs provide management and technical assistance to over 200,000 small businesses every year and training to over 300,000 business owners and their employees. These small business owners have the same basic question, "How do I succeed?". That's not always a simple answer but, for almost every business that means maximizing sales, and we've been able to aid those clients to the tune of nearly 7 billion of new sales every year.

This is a great statistic, but it contains a hidden peril, cyber-crime. More and more of our clients, especially in rural areas do a lot of business online. Every single one of them is vulnerable, and they may not even know it. They may not even have a website but they are potential victims. Every time they run a credit card transaction, or answer their email they expose themselves and their customers to the risk of hacking, phishing and ransomware.

And the dangers go beyond e-commerce. Any business, whether a vendor or a contractor, is at risk if they are connected and have personally identifiable information or the potential to be an access point to others who do.

By now I assume everyone is aware of the alarming statistics about cyber-crime. Cybercrime costs the global economy about $445 billion every year, with the damage to business from theft of intellectual property exceeding the $160 billion loss to individuals. Fifty percent of small businesses have been the victims of a cyber-attack and over 60 percent of those attacked will go out of business.

Despite these facts many small businesses continue to ignore or avoid the risk. Many of our clients believe, "I don't do business online or I don't have any valuable information." Of course, the truth is exactly the opposite. Every time they take an order, swipe a credit card or send an email they put themselves and their customers at risk. Too often the concern is for customer privacy but corporate clients and vendors are at risk too.

Small business present cybercriminals with an easy way to gain access to customer credit card records and bank accounts, supplier networks and employee financial and personal data.

They want to do more and more business online but they have weaker online security. Or they use cloud services that don't have strong encryption. As a result, the small business can be a gateway to gain access to clients, business partners, and contractors and a backdoor into many large organizations. To a hacker, that translates into reams of sensitive data behind a door with an easy lock to pick. If a small business has any Fortune 500 companies as customers, they are an even more enticing target. These secondary attacks are now a regular problem for small business.

Small businesses are particularly vulnerable to email attacks mimicking their banks or other trusted institutions and citing an urgent need for account or some other vital information, and often multiple employees have access to that information. Further, business accounts do not enjoy the same protection against loss as consumer accounts—something many small-business owners do not discover until it's too late. Consumers are protected by regulations which limit their liability. Commercial accounts, however, are covered by the Uniform Commercial Code (UCC) and have lesser protections. As a result, few small businesses that are the victims of cyber theft ever recover their funds.

More than ever, sensitive data, intellectual property and personal information of small and medium sized firms are targeted by an ever increasing and sophisticated community of cybercriminals. Symantec has found that over the last several years there has been a steady increase in cyber-attacks targeting businesses with less than 250 employees.

And not all hacking is for financial gain. Three years ago, several businesses were simultaneously hacked and their websites were taken over by what appeared to be ISIS. Islamic State logos and Arabic script was plastered all over the sites for Montauk Manor in the Hamptons; Eldora Speedway in New Weston, Ohio; Dogwoods Lodge dog kennel in Des Moines, Iowa; Sequoia Park Zoo in Eureka, CA; Montgomery Inn in Montgomery, Ohio; the Moerlein Lager House in Cincinnati; and Elasticity, a vocational charity St. Louis, MO.

No financial information was stolen but imagine the time, effort and lost business for each of these firms. They had to rebuild their sites and try to rebuild client confidence. After all, if you knew a hotel had been hacked would you give them a credit card to hold a reservation?

At the SBDCs we have been working to spread awareness of all these threats to our clients. We offer training programs at most SBDCs and we are working to expand the coverage to the entire network, developing programs to not only advise and inform our clients but spread the information and training capacity throughout our networks.

In Idaho, in addition to training, the SBDC at Boise State operates a list-serve to help SBDCs share information and skills on the cybersecurity threat. In Florida, our network is collaborating with Ridge Global, founded by former DHS Secretary Tom Ridge, to develop a series of training videos on cybersecurity.

At the University of Texas at San Antonio (UTSA) SBDC/PTAC they created a Cybersecurity Awareness and Compliance Training Program. Key emphasis there is placed on compliance with Defense Acquisition regulations. They also conduct training through a Small Business Cybersecurity Training Academy (SBCTA) and other Cybersecurity Workshops.

SBDCs began developing these resources on our own over the last few years. My members recognized that, while they are advising and training their clients on the value of the web as a marketing and sales engine, they also needed to educate them on the dangers and pitfalls of the web.

On top of the organic efforts within the SBDC networks we are now working at the national level to help develop a national small business cyber assistance. Pursuant to section 1841 of the National Defense Authorization Act for 2017 America's SBDCs is working with the Department of Homeland Security (DHS) and the Small Business Administration (SBA) to develop a strategy to leverage the collective resources of DHS, SBA and the national network of SBDCs to provide the resources, training and assistance small businesses will need.

We will be working to share and improve cyber programs, enhance services and raise awareness of the threats. We want to help develop cost-effective, high- quality tools for small business and a network to share information and analysis on threats.

On behalf of our clients I want to thank the members of this committee for their efforts in getting that language included in the NDAA. The timing could not be more critical, the threats and the awareness of the threats has grown but at the same time so has the confusion. What steps do small businesses need to take? Do they need security software, a cyber specialist, certifications? What tools are effective, what certifications are valid?

SBDCs are developing and training small businesses on that first line of their cyber security needs, the internal focus of basic security practices. Teaching employees about the threats and weaknesses, helping them protect client and customer information. They are also working with small businesses to help them recognize and develop their own strategies and assessments of their needs.

Our members have developed some excellent education and it will grow stronger but, the harder effort is going to be assisting small businesses in dealing with the external demands of cybersecurity.

Commercial customers and big business will have growing demands on the cyber infrastructure of their small business suppliers. What certifications will they demand, what hardware? Who will supply these certifications, and at what cost? If we add federal procurement issues (already a complicated area) how will small businesses cope?

At America's SBDC we will be working hard to ensure that our clients have the best possible, most cost-effective tools. We know there is a potential for small business to be a back door.

On the government side we want to help small business be ready to meet the security concerns of federal contracting authorities. There are significant concerns that federal and state agencies will develop conflicting and potentially contradictory procurement regulations, derived from the best intentions regarding security and privacy, but having a negative effect on small business participation.

That is why America's SBDCs is glad to be working on this strategy with DHS, SBA and other agencies now. We want to help head off the confusion and provide training to ensure opportunity is not sacrificed for cybersecurity.

At America's SBDC we believe it important to be at the front of this effort, to develop a set of resources to enable small business participation through assistance and training, rather than having to play "catch up" with small businesses confused by a new regulatory framework. That is why we support the Committee's legislative efforts.

Chairman Risch and Senator Peters are to be commended for their work on S. 2735, *the Small Business Advanced Cybersecurity Enhancements Act of 2018*.
This legislation will continue the work SBDCs have started with DHS and SBA sharing information and working to make that information more easily available to small business.

It will also help SBDCs make sure, by working with our federal partners, that our small business clients have the best resources and tools possible. We believe that while we have made a good start, this legislation will strengthen the cooperation and focus needed to bring small businesses the cybersecurity resources they need in the 21st century.

We'd also like to express our support for S 1428, the Small Business Cyber Training Act. We appreciate this recognition of the role SBDCs have as the front line of cyber-security training and advising. We look forward to working with the Committee to ensure that these bills give SBDCs the tools and flexibility they need to provide their small business clients with the best help possible.

Thank you again for the opportunity to testify on behalf of America's SBDCs.

○